Policy Contents

Policy Information

Effective Date:
March 1, 1998
Last Revised Date:
February, 2022
Policy Number:
Fin-300
Responsible Unit:
Records & Archives
Email:
records@fso.arizona.edu [1]

Purpose and Summary

This Policy clarifies the applicability of law and of other University of Arizona (University) policies to electronic mail (email), and also sets forth new policies uniquely applicable to email.

The University recognizes that principles of academic freedom, freedom of speech, privacy, and confidentiality hold important implications for email and email services. This Policy addresses these principles within the context of, and subject to, the limitations imposed by the legal and policy obligations of the University.

The purpose of this Policy is to ensure that:

1. Email is used by the University community in an ethical and considerate manner in compliance with applicable law and policies, including policies established by the University and its operating units, and with respect for the public trust through which these facilities are provided;
2. Email users are informed about how concepts of privacy and security apply to email, as well as the applicability of relevant policy and law; and

3. Disruptions to University email and other services and activities are minimized.

Scope

This Policy applies to:

1. All email services provided, owned, or funded in part or in whole by the University;
2. All users and holders of University email systems or accounts, regardless of intended use; and
3. All University email Official Records and/or Public Records in the possession of, or generated by, University employees and other users of email services provided by the University, regardless whether the records were generated on University or non-University computers.

This Policy applies equally to transmission and receipt data, including email headers, summaries, and addresses associated with email records, and any attached files or text.

This Policy does not apply to

1. Internet services other than email
2. Voice mail
3. Audio and video conferencing
4. Facsimile messages

This Policy does not apply to printed copies of email, but other law and policy may apply to such documents. Under Arizona records law and other state laws, information appearing in this format may need to be retained as Official Records or treated as State Publications under A.R.S. section 39-101, *et seq*. If the user prints out email Official Records (including transmission and receipt data) and retains them in hard copy according to approved University records management policies and retention schedules, the electronic copy may be deleted immediately. **(See Records & Archives Retention Schedule Policy [2] for related definitions and state-mandated guidelines on the storage and disposal of email records, or contact the University Records & Archives Department for instructions.)**

Policy

I. Specific Use Provisions

Provision of Service: Official University email is provided to all faculty, staff, and students by University Information Technology Services (UITS) in support of the University threefold mission of instruction, research, and public service. UITS additionally provides email to Designated Campus Colleagues upon request. Email accounts may also be provided by individual departments.

University Property: Email services are extended for the sole use of University faculty, staff, students, and other appropriately authorized users to accomplish tasks related to and consistent with the mission of the University. University email systems and services are University facilities, resources, and property as those terms are used in University policies and applicable law. Any email address or account assigned by the University to individuals, sub-units, or functions of the University is the property of the University.

Authorized Service Restrictions

1. Email users are required to comply with state and federal laws, University policies, and

standards of professional and personal courtesy and conduct. Access to University email services is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user: (a) when required by and consistent with applicable law or policy; (b) when there is a reasonable suspicion that violations of policy or law have occurred or may occur; or (c) when required to meet time-dependent, critical operational needs. Such access restrictions are subject to the approval of the appropriate University supervisory or management authority (e.g., department heads, systems managers, etc.). The autonomous operational units of the University must establish or identify these authority levels.
2. University operational units may define additional "Conditions of Appropriate Use" for local computing and network facilities to supplement this Policy with additional detail, guidelines, or restrictions. Such conditions must be consistent with and subordinate to this Policy, and are intended to deal primarily with situations of limited resource supply.
3. When an individual's affiliation with the University ends for purposes other than retirement or becoming Emeritus faculty, the individual's University official email service will be discontinued. Retirees may have the option to continue to use their University email address.

Authorized Access and Disclosure

1. The University may permit the inspection, monitoring, or disclosure of email when:
    a. required by or consistent with applicable law or policy such as Arizona Public Records law (A.R.S. section 39-121, regarding inspection of public records); the Family Educational Rights and Privacy Act (regarding access to student records); or any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on University systems to be accessed by authorized personnel in certain circumstances;
    b. there is a reasonable suspicion that violations of law or University policy have occurred or may occur;
    c. there are time-dependent, critical operational needs of University business if the University determines that the information sought is not more readily available by other means.
2. In such instances, the University will, as a courtesy, try to inform email users prior to any inspection, monitoring, or disclosure of email records, except when such notification would be detrimental to an investigation of possible violation of law or University policy. Users are required to comply with University requests for access to and copies of email records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate University personnel policies or Codes of Conduct.

Indemnification of the University: Users agree by virtue of access to the University computing and email systems, to indemnify, defend, and hold harmless the University for any suits, claims, losses, expenses, or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of University email and computing systems, services, and facilities.

II. Misuse

1. Using email for illegal activities is strictly prohibited. Illegal use may include, but is not limited to, obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications

system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark, or defamation law.
2. Failure to follow state law with regard to the disposition of email records may lead to criminal charges. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal, or secretion of email records may lead to class 4 or class 6 felony charges under A.R.S. section 38-421.
3. In addition to illegal activities, the following email practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this Policy; altering email system software or hardware configurations; or interfering with the work of others or with University or other computing facilities.
4. If a user is requested by another user via email or in writing to refrain from sending email messages, the recipient is prohibited from sending that user any further email messages until such time as they have been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this Policy. This provision does not apply to email messages required for the performance of job duties.
5. University email services may not be used for commercial activities not approved by appropriate supervisory University personnel consistent with applicable policy; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section III of this Policy; uses that violate other University policies or guidelines; or uses inconsistent with applicable state or federal law. Applicable University policies include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or discrimination and harassment.
6. Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the University of Arizona."
7. University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, strain on any computing facilities or interference with others' use of email or email systems. Such uses include, but are not limited to, the use of email services to:
    a. Send or forward chain letters.
    b. "Spam"; that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.
    c. "Letter-bomb"; that is, to resend the same email repeatedly to one or more recipients.

III. Personal Use

University email services may be used for incidental personal purposes provided that such use does not:

1. Directly or indirectly interfere with the University operation of computing facilities or email services.
2. Interfere with the email user's employment or other obligations to the University.
3. Violate this Policy, or any other applicable policy or law, including but not limited to, use for personal gain, conflict of interest, harassment, defamation, copyright violation, or illegal activities.

Email messages arising from such personal use shall, however, be subject to access consistent with this Policy or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

IV. Confidentiality

1. The confidentiality of email cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this Policy, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that their email is private or confidential.
2. Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, regardless whether the information is maintained on paper or is found in email or other electronic records.
3. The Office of the Registrar may elect to publish student email addresses as directory information, consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). Individual students may, consistent with University policy and FERPA, request the University not to treat the address as directory information. Requests for identification or release of students email addresses should be directed to the Office of the Registrar.

V. Security and Preservation

1. Email users and operators must follow sound professional practices in providing for the security of email records, data, applications programs, and systems programs under their jurisdiction.
2. Users and operators must guard against storage media deterioration and email record inaccessibility due to hardware or software obsolescence. To eliminate these situations, users must make provision for future accessibility by:
    a. migrating all official email records to the next generation of hardware or software; or
    b. migrating only current official email records to new hardware or software, or converting official email records not migrated to other media (e.g., optical disk, COM) for short-term storage or to "eye readable form" (i.e., paper or microfilm) for long term storage and preservation. (**See Common Retention Schedule** [3] **for state-mandated guidelines on the storage and disposal of email records, or contact the University's Records & Archives Department for instructions.)**
3. Users are responsible for safeguarding their identification (NetID) code and password, and for using them only as authorized. Each user is responsible for all email transactions made under the authorization of their NetID, and for all network email activity originating from their data jack. Use of email user identifications for commercial purposes is prohibited. Access to user identifications may not be loaned or sold.
4. Each operational unit should establish:
    a. Standards for official email records identification and file organization.
    b. Measures for protecting sensitive official email stored electronically.
    c. Procedures for file backup.

VI. Violations

Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate University authorities and/or law enforcement agencies. Violations may result in revocation of email service privileges; academic dishonesty or Code of Conduct proceedings; faculty, staff, or student disciplinary action up to and including dismissal; referral to law enforcement agencies; or other legal action.

VII. Online Policies

Users of this Policy are encouraged to refer to online versions of this and other University policies at University Policies website.

Appendix A: General Use Cautions [4]

Appendix B: Model Informational Handout Regarding University Email Policy [5]

Compliance and Responsibilities

Records & Archives Department

University Information Technology Services (UITS)

All users and holders of University email systems or accounts to whom this Policy applies are responsible for becoming familiar with and following this Policy.

University supervisors are responsible for promoting the understanding of this Policy.

University supervisors and appropriate University authorities are responsible for taking appropriate steps to help ensure compliance with this Policy.

Sources*

Family Educational Rights and Privacy Act

Arizona Revised Statutes § 39-103. Size of public records; exemptions [6]

Arizona Revised Statutes § 39-121. Inspection of public records [7]

Related Information*

1. All policies applied generally at the University are expressly applicable to the electronic environment. Relevant institutional policies include, but are not limited to:

- Arizona Board of Regents Policy Manual
- University Handbook for Appointed Personnel
- Classified Staff Human Resources Policy Manual
- All Codes of Conduct and Academic Integrity
- Confidentiality of Student Records
- Nondiscrimination and Anti-Harassment Policy
- Outside Professional Activity
- Conflicts of Interest and Commitment Policies
- Copyrights and Patents
- Use of University Name or Trademarks

2. This is not a comprehensive list of applicable University policies. Any policy which applies to the use of University resources, including equipment and time, also applies to email. In the event of a conflict between policies, the more restrictive use policy shall govern.

Revision History*

03/08/2022: Updated Records & Archives email address

02/24/2022: this revision includes:

1. Policy Section I: Provision of Service; Authorized Service Restrictions, paragraph 3
2. Policy Section II: Misuse, addition of third sentence at end of paragraph 4
3. Compliance and Responsibilities

03/01/1998: New Policy

Links
[1] mailto:records@fso.arizona.edu [2] http://rmaa.arizona.edu/retention [3] http://www.rmaa.arizona.edu/retention [4] http://policy.arizona.edu/appendix-general-use-cautions [5] http://policy.arizona.edu/appendix-b-model-informational-handout-regarding-university-e-mail-policy [6] https://www.azleg.gov/ars/39/00103.htm [7] https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/39/00121.htm