# Email Policy

## POLICY INFORMATION


**Policy Sponsor(s):** Elliott Cheu

Chief Information Officer

**Responsible Unit(s):** Office of the Chief Information Officer

**E-mail:** cio-comm-mar@arizona.edu


## Purpose and Summary

The University of Arizona (University) recognizes that principles of academic freedom, freedom of speech, privacy, and confidentiality are important for email, and the University Community needs to understand their rights and responsibilities when using University email. The purpose of this Policy is to outline these rights and responsibilities.

## Scope

This Policy applies to members of the University Community who are provided email that is owned or funded in part or in whole by the University. University email includes, but is not limited to, a University Email Account.

## Definitions

**Constituent** means anyone with whom the University has a relationship, including, but not limited to, prospective and current students, Employees, Designated Campus Colleagues (DCCs), alumni, parents and families, donors, business leaders, stakeholders, partners, and other members of the community.

**Designated Campus Colleagues (DCCs)** means affiliates, associates, volunteers, and interns who are granted DCC status by the University, who contribute their time, services, and expertise to help the University accomplish its mission of teaching, research, and service.

**Emeritus Faculty** means someone who has been granted Emeritus status from the Office of the President.

**Employee** means all University employees, including faculty, staff, graduate assistants/associates, and student workers, whether their employment is full-time, part-time, permanent, or temporary.

**Retiree** means someone who retired from the University and was granted a retiree status from Human Resources.

**University Community** means, for the purpose of this Policy, all University Employees, DCCs, Retirees, and Emeritus Faculty.

**University Email Account** means an email account in which the address is the NetID with @arizona.edu or any other variation that is assigned and used by the University Community.

**Unit** means any University college, school, department, program, or other operating unit.

## Policy

A. **Specific Use Provisions**

1. **Provision of Email**

a. In support of the University's mission of instruction, research, and service, University Information Technology Services (UITS) provides University Email Accounts to the following:
   i. Employees.
   ii. Emeritus Faculty.
   iii. Some classifications of DCCs.
   iv. Retirees who opt in to retain their University Email Account.

2. **Property of the University**

a. University Email Accounts are provided for the sole use of Employees and other appropriately authorized users to accomplish tasks related to and consistent with the mission of the University. Any email through University Email Accounts consists of University computing facilities, resources, and property as those terms are used in University policies and applicable law. Any email utilizing a University Email Account is the property of the University including transmission and receipt of data, email headers, email summaries, email addresses associated with email messages, and any attached files or text, regardless of whether the emails are generated on University or non-University workstations, devices, and network infrastructures.

B. **Use of Email**

1. Email communication is intended to meet the academic and administrative needs of the University and is used to communicate to the University Community regarding official business.

2. Employees are expected to use University Email Accounts for all official University business.

3. All members of the University Community must follow applicable state and federal laws and regulations governing the appropriate use and confidentiality of Constituent information, such as CAN-SPAM, FERPA, and HIPAA.

4. Employee email addresses are included in the University Campus Phonebook to facilitate communication among the University Community.

5. Employees are expected to check their email on a frequent and consistent basis to stay current with University-related communications.

6. The University Community is responsible for using or interacting with University email in a lawful fashion. The University requires individuals who are assigned a University Email Account to compose their email correspondence in a manner that follows standards of professional conduct as outlined in

the University Staff Standards of Professional Conduct Policy, Professional Conduct Policy, Classified Staff Rules of Conduct Policy, and Student Worker Rules of Conduct Policy.

C. **Terminating Access to Official University Email Account Upon Separation**

1. Employees who separate from the University for purposes other than retirement or becoming Emeritus Faculty will lose access to their University Email Account and use of their University email address upon separation.

D. **Continuation of University Email Account upon Retirement or Emeritus Status**

1. Retirees may opt in to retain use of their University Email Account.

2. Emeritus Faculty automatically retain their University Email Account when granted Emeritus status.

E. **Automatic Forwarding of Email**

1. University Community members are prohibited from automatically forwarding their email from a University Email Account to a non-University Email Account.

F. **Personal Use of University Email**

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

    a. directly or indirectly interfere with the University operation of computing facilities or email;

    b. interfere with the email user's employment or other obligations to the University; and/or

    c. violate this Policy or any other applicable policy or law, including, but not limited to, the Misuse of University Assets Policy, Conflicts of Interest & Commitment Policy, Nondiscrimination and Anti-Harassment Policy, Political Activity Policy, or copyright laws.

G. **Authorized Email 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 is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the email user when (a) required by and consistent with applicable law or policy; (b) there is a reasonable suspicion that violations of policy or law have occurred or may occur; or (c) 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.).

H. **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 (FERPA), 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; or

b. there is a reasonable suspicion that violations of law or University policy occurred or may occur; or

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, attempt to inform email users prior to any inspection, monitoring, or disclosure of email, 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 emails when access or disclosure is required or allowed by applicable law or policy, regardless of whether such emails 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.

I. **Misuse of University Email**

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. 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 the University or other computing facilities.

3. University email will not be used for the following:

a. commercial activities not approved by University supervisory personnel consistent with applicable policy;

b. personal financial gain (except as permitted under University policies, including the Conflicts of Interest & Commitment Policy);

c. any University Community member advocating for or against proposed legislation or Influencing the Outcome of Elections, as defined by the Political Activity Policy;

d. personal use inconsistent with Section F of this Policy;

e. uses that violate other University policies or guidelines, including, but not limited to, policies and guidelines regarding personnel, intellectual property, or discrimination and harassment; or

f. uses inconsistent with applicable state or federal law.

4. University email will 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. Such uses include, but are not limited to:

a. Chain letters being sent or forwarded;

b. Spam, meaning the exploitation of listservs or similar systems for the widespread distribution of unsolicited email; and

c. Email bombs, meaning identical emails that are resent repeatedly to one or more recipients.

J. **Confidentiality**

1. The confidentiality of email cannot be assured. Therefore, users should exercise extreme caution in using email to communicate confidential personal, financial, or sensitive matters over the network, 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 of whether the information is maintained on paper or found in email or other electronic transmissions.

K. **Records and Retention of Email**

1. If an email is determined to be a Record of the University, as defined in the Record Retention and Destruction Policy, the email in its entirety (all metadata, attachments, distribution information, etc.) must be securely stored and retained for the proper period of time based on its assigned record series type found in the retention schedules used by the University. Once all retention guidelines have been met and the email Record no longer has any additional administrative, legal, research, or historical value, the email Record can be destroyed by following the proper record destruction procedures. For more information about record retention schedules or applicable email record guidelines, consult with the University Records & Archives Office.

L. **Violations**

1. Suspected or known violations of this Policy or related laws should be reported to the appropriate supervisory level for the Unit in which the violation occurs or the Ethics and Compliance Hotline. Violations will be processed by the appropriate University authorities and/or law enforcement agencies. If the violation involves an information security issue or requires technical assistance, the appropriate University official will engage the Information Security Office or University Information Technology Services as needed. Violations may result in revocation of email privileges; academic dishonesty or code

of conduct proceedings; faculty, staff, or student disciplinary action; referral to law enforcement agencies; or other legal action.

## Compliance

The Office of the Chief Information Officer is responsible for overseeing compliance with this Policy.

Please note that the following sections are provided solely for the convenience of users and are not part of the official University policy.

## Sources

A.R.S. section 39-121 Inspection of Public Records

ABOR Policy 5-301 Code of Conduct

ABOR Policy 6-914 Protection of Employees from Reprisal for Whistleblowing

Electronic Communications Privacy Act of 1986

Family Educational Rights and Privacy Act

## Related Information

Acceptable Use of Computers and Networks Policy

Approved Use of University Computing and Communication Equipment Policy

Classified Staff Rules of Conduct Policy

Conflicts of Interest & Commitment Policy

Email Record Guidelines

Ethics and Compliance Hotline

Misuse of University Assets Policy

Nondiscrimination and Anti-Harassment Policy

Political Activity Policy

Professional Conduct Policy

Record Destruction Procedures

Record Retention and Destruction Policy

Record Retention Schedules

Retirement Policy

Retiring Faculty Resources – Emeritus Status

Student Worker Rules of Conduct Policy

University Records & Archives Office

University Staff Standards of Professional Conduct Policy