Responsible Executive: Chief Information Officer
Responsible Office: Information Security Services
Effective Date: December 30, 2019
Last Revised: TBD

ELECTRONIC MAIL

POLICY SUMMARY

Northern Arizona University's electronic mail (or "email") service is a tool intended to support the University's official educational, administrative, and business activities while providing an official means of communication between the University and its employees and students. Except for minor incidental personal activity, use of the University's email systems must further the University's mission while complying with applicable law and policy. All users are advised that email transmitted or stored by the University may be accessed, reviewed, or disclosed to appropriate third parties in accordance with applicable law, policy, or legal order. While the University endeavors to provide a secure and dependable email service, users must exercise caution when communicating confidential or sensitive information and should be aware that, with some exceptions, the content of University email accounts is generally subject to disclosure under Arizona's public records laws.

REASON FOR THIS POLICY

Prudent administration of the University's email services requires articulation of the system's appropriate uses, Authorized User privileges and responsibilities, and related matters. This also promotes institutional efficiency and effectiveness, enhances individual accountability, and helps to mitigate risk.

ENTITIES AFFECTED BY THIS POLICY

- All University units at all locations

WHO SHOULD KNOW THIS POLICY

- All persons assigned an NAU email address (or another email address controlled by the University)
- Chief Human Resources Officer
- Dean of Students
- Executive, department, and academic leaders, including deans, associate deans, chairs, and directors
- Chief of Staff
- Provost and Vice President for Academic Affairs
- Vice Provost for Academic Personnel

DEFINITIONS

Authorized User: a person who has truthfully identified themselves and their purposes and to whom the University has granted access credentials to permit their Authorized Use of the University's IT Resources, or a person accessing the University's public information services through a network connection open to the general public, for legitimate activity or purposes that further the University's mission.

University Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University. These resources are referred to herein as "University IT Resources."

POLICY

A. Scope and Applicability

This policy applies to all Northern Arizona University email communication services, including Instant Messaging, and all those assigned an NAU email address, or another email address controlled by the University, and related account access. All Authorized Users are responsible for knowing and complying with this policy. Use of an assigned NAU email account evidences the Authorized User's agreement to be bound by and to comply with this policy and all other applicable requirements and standards. This policy supplements and extends, but does not supersede or replace, the University's *Safe Working and Learning Environment* policy, the *Student Code of Conduct*, and the *Appropriate Use of Information Technology Resources* policy and its accompanying *Standards for the Appropriate Use of Information Technology Resources*. In the event of a conflict or inconsistency between this policy and any of the aforementioned policies, the aforementioned policies will prevail. This policy is not intended to and may not be used to curtail the First Amendment rights of University Community Members. The University will enforce this policy in a manner consistent with constitutional freedom of speech protections.

B. General

Use of the University's email system is a privilege granted to Authorized Users in furtherance of their educational opportunities or professional responsibilities, contributions, or achievements. Every Authorized User bears the responsibility to use or interact with the University's email services in a lawful and ethical fashion. The University expects its employees to compose their email correspondence in a manner that comports with normal standards of professionalism.

C. Personal Use

Incidental personal use of employee email accounts is permitted, provided that such occasional use complies with applicable law and policy and does not adversely impact work responsibilities or network performance. Use of NAU email accounts provided to retirees in recognition of their contribution to the University may be for personal purposes, but such personal use must continue to comport with all applicable laws, policies, or other requirements. Following their separation from the University, students, employees, and retirees may have no expectation of access to their University email accounts or the information they contain beyond that described in this policy (in particular, see Sections I and M). All personal use described above is subject to University monitoring, inspection and disclosure as established by this policy and applicable law. Thus, no reasonable expectation of privacy applies or attaches to such personal correspondence or information which uses the University's IT Resources or infrastructure.

D. Ownership and Administration

1. The University owns and controls all University-provided NAU email addresses, aliases, and accounts. Subject to underlying copyright, intellectual property, or other rights established by applicable law and policy, the University also owns all electronic data and information created, transmitted, or stored using these University email accounts and related Instant Messaging services. University email addresses and email aliases may be reclaimed or otherwise reassigned based upon university provisioning requirements and do not belong to an individual.

2. When necessary to protect or resolve a threat to Authorized Users or the University's IT resources or infrastructure, or to prevent or respond to a violation of law or policy, the University may, without notice, take actions necessary to manage or address such situations and to preserve the integrity of its electronic data, including email records. Such actions may include, but are not limited to, changing passwords, rescinding access rights, disabling or impounding University-owned computers, or disconnecting specific devices or segments of the University's network.

3. If the same email account is compromised multiple times, Information Technology Services may disable the account until remediation is accomplished and the Authorized User completes remedial information technology security training. Authorized Users are required to fully cooperate and comply with any investigation of real or perceived abuse or misuse of University email.

~~E. Email Conventions~~

- ~~The University shall automatically generate email addresses and email aliases for University Community Members based upon their name or assigned NAU UID, and their role within the University. University Community Members may request additional email aliases for their university email account through an authorized process with the Information Technology Services department.~~
- ~~University managed shared mailboxes for departments, organizations, clubs, and other email accounts not directly associated with a singular University Community Member may be requested for use within the boundaries of University business.~~
- ~~Email accounts are prohibited from utilizing an email address or email alias to pose as, mimic, falsely identify, or otherwise conflicts with other reserved name spaces for individual email accounts, unless an exception request has been approved through Information Security Services.~~
- ~~University email addresses and email aliases may be reclaimed or otherwise reassigned based upon university provisioning requirements and do not belong to an individual.~~

F. Security, Access Credentials, Presumption of Authorship

While the University endeavors to provide secure and dependable email services, all users should exercise caution when using these services to communicate confidential or sensitive information. Each Authorized User is charged with protecting their account access credentials from loss or unauthorized use. Sharing one's access credentials with any person for any unauthorized reason or purpose is a violation of this policy subject to disciplinary action. The University will presume that all email correspondence originating from an account has been authored and transmitted by the account holder.

G. Prohibited Uses

The University's email system may only be used for legitimate or authorized purposes that further or comport with its educational mission and administrative activities. Unlawful or unauthorized uses may include, but are not limited to, harassment and intimidation of individuals based on race, color, national origin, sex, religion, sexual orientation, or disability; accessing, creation, display or transmission of obscenity or material harmful to minors as defined by law; true threats; theft; unauthorized attempts to gain access to data; attempted breaches of security measures; attempting to intercept electronic communication transmissions without proper authority; and violation of copyright, trademark, intellectual property, or defamation laws. Illegal use of the University's email systems will be reported to the appropriate law enforcement authority and may subject the offender to both civil and criminal liability. The University's *Appropriate Use of Information Technology Resources* policy and its accompanying *Standards for the Appropriate Use of Information Technology Resources* provide more information in this regard. The following is a non-exhaustive list, intended for illustrative purposes only, of behaviors that constitute violations of University policy:

1. Altering, disabling, circumventing, or interfering with any aspect of the University's email services;

2. Accessing or distributing email messages belonging to another person without authorization;

3. Intentionally distributing computer viruses, worms, Trojan horses, malware/ransomware, phishing, corrupted files or hyperlinks, hoaxes, or other items of a destructive or deceptive nature;

4. Using the University's email system to violate the University's *Standards and Expectations of Conduct*, *Student Code of Conduct*, or its *Safe Working and Learning Environment* policy;

5. Creating or using a false or alias email address to impersonate another person or altering email information to conceal or misrepresent one's identity or affiliation; or that conflicts with other reserved name spaces for individual email accounts;

~~5.~~6.

~~6.~~7. Creating or intentionally disseminating spam, chain letters, or "letter-bombs" (where a message is resent to the same email address(es) repeatedly) or other unauthorized bulk mailings for a purpose that conflicts with the University's mission;

~~7.~~8. Transmitting unauthorized surveys or survey participation requests in violation of the University's *Conducting University Surveys* policy;

~~8.~~9. Promoting or engaging in unauthorized commercial or business activity for personal gain or otherwise, or for fundraising or promoting organizations not legitimately associated with the University;

~~9.~~10. Employee engagement in political activity, such as by attempting to influence the outcome of any election or to advocate in support or opposition of pending or proposed legislation, in violation of Arizona Board of Regents Policy 6-905 and Human Resources Policy 5.10;

~~10.~~11. Intentionally distributing software intended to covertly gather or transmit information; or

~~11.~~12. Testing or attempting to reverse-engineer the University's email system in order to discover its security vulnerabilities or to evade its filtering capabilities.

H. Using Personal Email for University Business

To avoid confusing business and personal communications and to support University compliance with applicable public records and record retention laws, University employees are prohibited from using personal email accounts or deploying non-University email systems or accounts to conduct University business or to meet their professional duties or responsibilities. For example, faculty must not use personal email accounts to communicate with their students. Although minor incidental personal use of University email accounts is permitted, employees should nonetheless avoid using NAU email to conduct their personal affairs (*e.g.*, creating service or billing account log-in credentials with NAU email addresses).

I. University Access

Under certain circumstances, including, but not limited to, performing system maintenance or recovery, investigating security breaches, threats, or reasonably suspected violations of this or other applicable policy, or complying with legal requirements, it may be necessary for the University to access, inspect, review, or monitor a University email account's activity or content. Email accounts belonging to individuals who will not or can no longer access the account may also be accessed and their contents disclosed as described in Section I.

J. Disclosure

1. Authorized Users should be aware that, with some exceptions, the University's email records are generally subject to disclosure under Arizona's public records laws. Further, the University may be compelled to monitor or disclose email correspondence or associated data in response to various legal or policy mandates, including, but not limited to, investigations, search warrants, court orders, or subpoenas. The University will monitor, inspect, or transmit to an authorized third-party email system content, activity, device identification, or related data as necessary to fulfill its legal obligations and to effectively administer its email system and other information technology resources. The University may use email content or related data in furtherance of employee or student disciplinary proceedings.

2. The content of University email account holders who can no longer access the account for reasons including, but not limited to, death, disability, incapacitation, illness, investigation, or separation from the University may be accessed by the University as necessary and appropriate. The University will disclose the content of such accounts only to properly authorized officials or third parties who have a legitimate right to the information. Those seeking to obtain University-held data associated with a deceased or incapacitated person may use the Request Another's University-Held Data Form to initiate such a request.

K. Email as an Official Means of Communication

The University considers its NAU email services to comprise an official means of communication with its employees, students, affiliates, and agents. The University depends upon its email system to electronically transmit important information, including for all faculty who are on contract. Authorized Users are responsible for accessing their email in a timely manner, as the University deems materials transmitted to NAU addresses to have been delivered to and received by the intended recipient(s) on the day of transmission. When they are unable to do so, faculty and staff should implement an automated "Automatic Reply" to indicate that they are unable to receive email communications for the relevant period. While email is an official means of

communication, it is not the only official means of communication and does not preclude the University's use of other methods.

L. Electronic Financial Aid Transactions

Students must affirmatively consent in order to conduct federal financial aid transactions with the University and to receive related notices via their NAU email accounts. Students who do not consent understand that they: i) will not be able to submit financial aid information online; ii) must submit financial aid documents in hard-copy form, which will extend processing time; iii) may not receive electronic reminder notices about financial aid disbursements or related matters. Students can update their financial aid consent preferences at any time.

M. Email Privileges Following Separation

When an individual's active affiliation with the University ends, the individual's University email privileges will continue or terminate in accordance with the requirements set forth below. Notwithstanding these provisions, the University reserves the right to revoke any Authorized User email privileges at any time should a member of the President's Executive Team, with the concurrence of the Chief of Staff, determine that doing so is in the University's best interests. Personal use of University email accounts by retirees must continue to comply with the University's *Appropriate Use of Information Technology Resources* policy and its *Standards for the Appropriate Use of Information Technology Resources*. University email privileges do not extend to employee or retiree family members, representatives, or those who are no longer living.

1. Faculty who separate before retirement. Absent good cause to the contrary, as determined in writing by the Provost, all faculty (faculty includes, for this purpose, all faculty on administrative assignment, including, but not limited to, chairs, associate deans, deans, vice provosts, and the Provost) who voluntarily separate from the University before retirement shall, as a means of accommodating the academic calendar, retain their NAU email privileges for one hundred eighty (180) days following their date of separation. The NAU email privileges of faculty who involuntarily separate from the University shall terminate in accordance with instructions provided by the Vice Provost, who shall notify Information Technology Services accordingly.

2. Staff who separate before retirement. Absent good cause to the contrary, as determined in writing by the Chief of Staff, the NAU email privileges of administrators, service and academic professionals, and classified staff members who separate from the University before retirement, whether voluntarily or involuntarily, shall terminate no later than two fourteen (14) days after their last day of employment. Application of this provision excludes student workers and graduate assistants, who shall retain their student email privileges in accordance with Subsection 6.

3. Retired faculty. Absent good cause to the contrary, as determined in writing by the Provost, faculty who retire from the University shall, upon request, retain their NAU email privileges.

4. Emeritus faculty. Absent good cause to the contrary, as determined in writing by the Provost, faculty who are awarded emeritus status shall, upon request, retain their NAU email privileges.

5. Retired staff. Absent good cause to the contrary, as determined in writing by the Chief of Staff in consultation with university officials, administrators, service and academic professionals, and classified staff who retire from the University shall upon request retain their NAU email privileges.

6. Students and alumni. Absent good cause to the contrary, as determined in writing by the Vice President for Student Affairs, students and alumni who receive a grade in at least one credit-bearing course shall retain their NAU email privileges.

7. Students who are expelled. The NAU email privileges of expelled students shall terminate no later than the date their expulsion becomes final, as directed by the Dean of Students, who shall notify Information Technology Services accordingly.

8. Agents or Affiliates. Absent good cause to the contrary, as determined in writing by a member of the President's Executive Team, University email privileges enjoyed by any University agent or affiliate shall

terminate upon either a predetermined expiration date, the completion of their work, or their separation from the University.

N. Inactive Accounts

The University reserves the right to periodically delete any NAU email account that remains unused or inactive for any period in excess of six (6) months, following thirty (30) days of advance notice.

O. Record Retention

It is mandatory that employees preserve University records, including emails, in the following circumstances:

1. They possess knowledge of matters or control information where litigation is reasonably anticipated or already occurring;

2. A subpoena has been served or notice of the intent to subpoena the material has been provided; and

3. The records are sought pursuant to an internal or external audit or a similar pending or reasonably anticipated possible investigation.

~~E.~~P. Phishing

1. Phishing is the process of using fraudulent email to acquire sensitive information. This is accomplished by masquerading as a legitimate or trusted entities to trick the recipient into providing personal information such as usernames, passwords, multifactor authentication codes, bank account information, Social Security numbers, or credit card information.~~This is accomplished by masquerading as a legitimate or trusted entity to trick the recipient into providing personal information such as usernames and passwords, bank account information, Social Security numbers, or credit card information.~~ In most cases, phishing scammers are seeking something of monetary value or to commandeer computers or user accounts. Responding to a phishing scam can result in identity theft, whereby a criminal may successfully apply for credit in another's name, empty another's bank account, or use another's email account to send spam or more phishing attacks to others. Phishing attacks can be very convincing and are often designed to mimic legitimate entities, such as the University itself, banks, service providers, or government agencies.

~~2.~~ Authorized Users should protect themselves and the University from phishing attacks by treating all unsolicited emails that request personal information with extreme caution and skepticism.~~ Authorized Users~~ University Community Members ~~should~~ must not intentionally click on any suspicious email, link, or file, unless they have been duly authorized by the CIO, or their designee~~never click on links in emails of uncertain origin or provenance and should not open any attached files~~. Authorized Users should only provide their NAU Credentials to NAU authorized services. To ensure Authorized Users only access NAU authorized services they should not follow links provided by unverified or untrusted sources. Authorized Users should report, via approved NAU phish reporting methods, any suspected or legitimate phishing attempts they encounter. Per the University's Access Policy, if ISS suspects a University Community Member has clicked on a suspicious link ISS, in their discretion, may secure the account associated with the click. ~~Authorized Users should always, via their browser, go to their service provider's web page directly before logging in or entering any personal information and should use the University's Phish Report Application to report all phishing attempts~~. This will help Information Security Services address the threat. Employees should note that the employee—not the University—is responsible for any personal financial loss that results from the employee's failure to protect their University account access credentials from phishing or similar schemes, swindles, or hoaxes.

~~P.~~Q. Indemnification

Except for NAU employees acting within the course and scope of their NAU employment, Authorized Users agree by virtue of accessing or using the University's email services to indemnify, defend, save, and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents, and employees for, from, and against any and all claims, actions, liabilities, damages, losses, or expenses (including court costs, attorneys' fees, and costs of claim processing, investigation and litigation) for

bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by the Authorized User's: i) negligence, acts or omissions; ii) breach of this or any other applicable policy; or iii) a failure to comply with applicable law or contractual or licensing agreement rights or requirements.

~~Q.~~R. Compliance and Enforcement

1. All executive, department, and academic leaders, including deans, associate deans, department chairs, and directors, are responsible for using all appropriate communication channels and other means to help ensure that all staff, faculty, and students are aware of the contents of this policy.

2. The University reserves the right to suspend network access and examine any email account pending additional proceedings organized in accordance with the *Appropriate Use of Information Technology Resources* policy and *Standards for the Appropriate Use of Information Technology Resources.*

3. Violations of this policy are subject to disciplinary action up to and including termination or expulsion. As with all University IT Resources, misuse of the University's email systems may result in the temporary or permanent revocation of access privileges and potential civil liability and/or criminal prosecution.

R. Authorized Systems

Authorized Users accessing their NAU issued email account should only use authorized clients provided and supported by Information Technology Services such as Outlook, Outlook for Web, and Outlook Mobile for employees and Gmail (website and mobile) for students. Employees must refer to the Device Configuration Policy regarding personal devices being used to access University data (such as email).

Use of third-party systems by faculty, staff, employees, and affiliates as an intermediary for accessing email is not permitted, unless an exception request has been approved through the Information Security Services Office.

This includes but is not limited to:

- Forwarding email to a third-party email address
- Email aggregation services
- Downloading email into a third-party email account
- 3rd-party integrations that require SMTP
-

~~-~~Domains that are controlled or managed by NAU or send on behalf of NAU must have published DMARC policies that define how email should be authenticated. All systems or services that send email on behalf of NAU controlled domains must abide by those policies. Those policies should be as restrictive as possible to prevent spoofing of NAU email addresses. Information Technology Services may assist with establishing a configuration that is secure and meets the policies. Systems or services that send mass email to external email addresses should use an nau.edu subdomain where possible.

RESPONSIBILITIES

Chief Human Resources Officer: respond to requests from staff members who wish to maintain their University email privileges following retirement.

Dean of Students: ensure that the University email privileges of expelled students are appropriately terminated no later than the student's official date of expulsion.

Executive, Department, and Academic Leaders: help to ensure that all faculty, staff, and students are aware of the contents of this policy.

Chief of Staff: respond to requests from staff who separate from the University prior to retirement who wish to maintain their University email privileges.

Vice President for Academic Affairs: determines whether Emeritus or retired faculty or former student or alumni University email privileges should be revoked due to misuse or abuse.

Vice Provost ensures that the University email privileges of faculty who are involuntarily separated from the University are appropriately terminated.

PROCEDURES

Use the Request Another's University-Held Data form to initiate a request to obtain the contents of a deceased or incapacitated student, faculty, or staff member's email account or other University-held data. Submit requests for student data to the Office of the Dean of Students, 1050 South Knoles Drive, Flagstaff, AZ, 86011 or via email to DeanofStudent@nau.edu. Submit requests for faculty or staff data to Human Resources, 411 South Beaver Street, Flagstaff, Arizona, 86011 or via email to HR.Contact@nau.edu.

RELATED INFORMATION

Forms or Tools

Request Another's University-Held Data

Cross-References

Affiliate Management

Appropriate Use of Information Technology Resources

Standards for the Appropriate Use of Information Technology Resources

Conducting University Surveys

Data Classification and Handling

Human Resources Policy 5.10

Responding to a Student Death

Standards and Expectations of Conduct

User Account Types

Sources

Arizona Board of Regents Policy 6-905

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

Arizona Revised Statutes Title 39 – Public Records

APPENDIX

None.