THE UNIVERSITY of NEW ORLEANS	**Policy No:**	**AP-AA-39.2**
	TITLE:	**Email Usage**
	EFFECTIVE DATE:	**March 1, 2019* (*Policy Revised, see below)**
ADMINISTERED BY: Office of the Provost and Senior Vice President for Academic Affairs	**CANCELLATION:**	
	REVIEW DATE:	**Fall 2024**

PURPOSE

The University of New Orleans' email services support the educational and administrative activities of the University to serve as a means of official communication by and between users and UNO. The University has the right to expect that such communications will be received and read in a timely fashion. The purpose of this policy is to ensure that this critical service remains available and reliable and is used for purposes appropriate to the University's mission and reputation

AUTHORITY

Part Two, Chapter III, Section I of the bylaws and rules of the University of Louisiana System.

SCOPE

This policy applies to all faculty, staff, students, student workers, retirees, sponsored accounts, guests and alumni who are assigned a UNO email account. In general, this policy applies to anyone who uses a @uno.edu email account.

GENERAL POLICY

Requirement to Use UNO Email

To be compliant with state regulations, all UNO employees (staff, students and faculty) must use the University-provided email system for official University communications to and among faculty, staff, and students. Employees must never use non-University email accounts (e.g. Gmail, Cox, etc.) to conduct University business to assure that work-related content is retained according to the published retention schedule. Automatic rule-based forwarding of emails to another email system is expressively prohibited.

Student workers should be aware that employee email accounts are issued to them when they are hired by UNO. These employee email accounts are separate and apart from their UNO student email accounts. Student workers are required to use their employee email accounts for their employment duties. Supervisors of student workers should inform student workers of their employee email

accounts when orienting them to their jobs. Supervisors should require student workers to periodically check their employee email accounts for work-related messages.

Email System Security and Privacy

UNO Email is designed to be protected by conditional multifactor authentication. However, email content is not encrypted. UNO will make reasonable efforts to maintain the integrity and effective operation of its email systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information.

Email users are advised that electronic data contained on the email system may be reviewed and/or accessed by authorized University officials for purposes related to University business, misuse, and unauthorized access or to protect against security threats such as cyber-attacks, malware, and phishing. The University may also access University email to conduct an official University investigation.

Furthermore, users are advised not to consider any of their e-mail or electronic communication correspondence on the University email system to be private.

EMAIL SECURITY THREATS

Email is increasingly being used by criminals, state and non-state actors to steal credentials, resulting in an invasion of the victims' professional and personal lives. Phishing attacks, extortion emails, intellectual property theft, confidentiality breaches, viruses and other malware are a constant threat that IT departments across the globe are facing. Stolen credentials can be used to further obtain University data, steal or extort money, spread chaos and confusion, and damage our reputation as an institution. It can also cause the University's email domain to have a "bad reputation" across the Internet, resulting in our legitimate emails being quarantined, filtered and/or flagged as spam at other institutions.

Legacy Email Clients

UNO is using modern authentication tools such as conditional multifactor authentication, and risk scoring to protect campus users from attacks. However, older email protocols such as POP3, IMAP, and SMTP do not work with multifactor authentication. As a result, attackers can use these older protocols as a vehicle to bypass our protections and encroach our Intranet. Future campaigns will help migrate campus users from these vulnerable protocols, and they will eventually be blocked completely.

Modern Email Clients

A non-exhaustive list of modern email clients are:

- Outlook for IOS and Android
- Outlook for PC and Mac
- IOS Email Client 11.4 or above
- Thunderbird
- Other third-party clients (i.e. BlueBird)

INAPPROPRIATE USE

Users must not:

- Automatically forward their UNO email to another email system.
- Test or reverse-engineer email services with the intent to find limitations, vulnerabilities or evade filtering capabilities.
- Send unauthorized marketing content or solicitation emails.
- Use email for partisan political or lobbying activities.
- Send insulting or discriminatory messages and content.
- Attempt to harass, trick, spam, or defame other people.
- Conduct business for personal profit under the aegis of the University for commercial or personal gain.
- Allow another person to use your email account.

This list is not intended to be exhaustive but rather to provide some illustrative examples of inappropriate use and etiquette.

RECOMMENDATIONS AND WARNING

- Use UNO email to conduct and communicate University business only.
- Sign up for newsletters, platforms and other online services that will help with academic or professional growth.
- Use an Email client that supports modern authentication.
- Set up multifactor authentication.
- Select strong passwords with at least ten characters (capital and lower-case letters, symbols and numbers) and avoid using personal or obvious information (e.g. birthdays).
- Abide by UNO's Acceptable Use for Information Technology (AP-AA-24).
- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing").
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks, requests for personal and/or financial information, etc.).

PERSONAL USE (Staff, Faculty and Student Workers)

- Incidental personal use of email is allowed with the understanding that the primary use be work or study related, and that occasional use does not adversely impact work responsibilities, security or the performance of the network.
- While the University will make every attempt to keep email messages secure, privacy is not guaranteed, and users should have no general expectation of privacy in email messages sent through University email accounts.
- The University does not guarantee nor accept the responsibility that all personal email sent to the UNO account will be received by the user. Due to security considerations and filtering, some personal email may be not allowed to be received into our system.

- Employees must keep operating systems and anti-virus programs updated while using personal computers and mobile devices used to access UNO email.

EMAIL SIGNATURE (Staff, Faculty and Student Workers)

It is important that all University communications are consistent with the University of New Orleans brand. Users must follow the instructions: http://www.uno.edu/University-marketing.

OUT OF OFFICE REPLIES (Staff, Faculty and Student Workers)

- Be courteous. It is important that each user exhibits professionalism in his or her dealings with students and colleagues, even in an automatically generated email message.
- Please make sure to set the correct end date, so people will not continue to receive automatic messages after you have returned.
- Please use out-of-office replies sparingly. They are not necessary to use every time you are away from your desk for a few hours or even for a full day, as long as you occasionally monitor your messages from a mobile device. Excessive use of these automatic replies gives the impression that we are unavailable and disinterested.

ENFORCEMENT PROCEDURES

A. **Complaints of Alleged Violations**. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established University Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the department overseeing the facility most directly involved who must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

B. **Reporting Observed Violations**. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the department overseeing the facility most directly involved. This department must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

C. **Disciplinary Procedures**. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, the Staff Handbook, the Student Handbook, and other applicable materials. Systems Administrators may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators are authorized to investigate alleged violations.

D. **Penalties**. Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violators may also face IT specific penalties, including temporary or permanent reduction or elimination of some or all

IT privileges (regardless of fees paid in the case of students). The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. **Legal Liability for Unlawful Use**. In addition to University discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. **Appeals**. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

John W. Nicklow
President
University of New Orleans

**Policy Updates:*
Revisions: 11/30/2021