Yeshiva University

EMAIL POLICY

The purpose of this Policy is to set forth the requirements and proper use of University email accounts by University administration, faculty and other staff. This Policy should be read together with other University policies, including the University's Technology Resources Use Handbook.

University Email as Only Means of Communication

All University administration, faculty and other staff should only use their University email accounts (@yu.edu) when conducting University business.

Only University email accounts should be provided on University websites, syllabi, business cards or other University documents.

The University's Learning Management System (LMS), and not email, should be used for student submissions.

University email should not be automatically forwarded to an external service provider.

Personal Use

Personal use of a University email account is permitted as long as it does not interfere with the University's needs or operations or with the user's work responsibilities to the University, and is otherwise in compliance with University policies. In no event, however, may a University email account be used for commercial activities, personal gain or political activities, or be used to represent the interests of a non-University group unless authorized by an appropriate University official.

Ownership and Privacy

The University owns all University email accounts. Users do not have a personal privacy right in their University email accounts. Emails may be reviewed and monitored by University personnel at any time and for any reason without user permission.

Retention

As provided in the University's Record Retention Policy, email should be mainly used as a form of messaging, and therefore should not be viewed as a long-term storage mechanism and generally should be deleted from email accounts within six (6) months. Accordingly, email messages and attachments subject to the University's Record Retention Policy generally should be saved from email accounts and stored in accordance with the user's department's policies within six (6) months of receipt, and thereafter such email messages and attachments should be deleted from the email account. If litigation is likely to be filed or has been actually filed, email messages and attachments relating to such litigation or potential litigation must be saved until the litigation proceedings are over. Please save relevant emails in accordance with the instructions of the University's Office of the General Counsel or other appropriate University officials.

Yeshiva University

Signatures

All University business-related emails must clearly identify the user by full name and official title. The user's telephone number and department signature with all appropriate disclaimers also must be included. (See Section 3.1a, E-mail Signature, of the Branding Guidelines on the Marketing and Communications website, https://www.yu.edu/sites/default/files/inline-files/_FINAL_YU_Branding_Guide3%202017.pdf.)

Security

Incoming emails are scanned for viruses, phishing attacks and spam, and suspected emails are blocked. However, it is impossible to guarantee protection, and each user must use proper care and consideration to prevent the spread of viruses etc. Attachments that are not clearly business-related and/or not expected from a known source should never be opened or executed.

Confidential Data

Sensitive and confidential data (such as social security numbers, credit card numbers, student grades and educational records, personnel records and health information) should only be transmitted through secure methods. Users must consult with the Information Security division of the University's Information Technology Services (ITS) department at infosec@yu.edu to determine the secure encryption method to use to email confidential data.

Passwords

Each user is responsible for his/her email account, including safeguarding of access, and should not share his/her password. Please see the University's Technology Resources Use Handbook for more information about the University's Password Policy, including password requirements.

Questions

Questions or comments about this Policy should be directed to the Information Security division of the University's Information Technology Services (ITS) department at infosec@yu.edu.

Yeshiva University

General Guidelines for Sending Emails

Users should:

- Compose emails with care and precision to properly reflect the University.
- Spell-check all emails prior to sending.
- Avoid any statements that could be viewed as defamatory or slanderous or otherwise unlawful or contrary to University policies.
- Avoid using ALL CAPS.
- Sparingly use **bold** and *italics*.
- Consider if an email is the most appropriate form of communication, especially if the message is intended to be confidential.
- Select the recipients cautiously, and do not add recipients to the "to," "cc," or "bcc" lines without careful consideration.
- Do not overuse Reply to All. Only use Reply to All if you really need your message to be seen by each person who received the original message.
- Check the recipient's email address to ensure that it does not contain any error.
- When sending a reply email or forwarding an email, avoid including the list of email addresses from the original email, and check the email series and any attachments to make sure that it is appropriate to share the content with the new recipient.
- Compress attachments larger than 1 MB before sending them.

Users should not:

- Intentionally distribute spam, phishing, chain letters, or similar communications.
- Transmit material in a manner which violates any intellectual property, copyright and other laws.
- Violate, or encourage the violation of, the legal rights of others, or federal, state or local laws.
- Alter, disable, interfere with, or circumvent any aspect of the email services.
- Forge, or attempt to forge, email messages.
- Disguise, or attempt to disguise, his or her identity when sending emails.
- Send or receive email messages using another person's email account.
- Attempt to access another person's email to which he or she does not have authorized access.
- Send any message which may be deemed to constitute unlawful harassment (including sexual harassment).
- Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks.