1.0 Purpose

The purpose of this policy is to ensure that Montclair State’s electronic mail (e-mail) services remain available to and reliable for the University community, and are used for purposes appropriate to the University’s mission.

2.0 Scope

This policy applies to all members of the Montclair State community who are entitled to email services.

3.0 Policy

3.1 Use of Montclair State University Email Addresses and Accounts

For the duration of time that an individual is an official, active member of the Montclair State community (enrolled student, employee, active faculty) email is the official means of electronic communications to that individual. As such, official University communication mechanisms (including but not limited to: email to the allusers and allstudents lists, course email, and email from University departments) should be read on a regular basis since they may affect day-to-day activities and responsibilities.

The Information Technology Division provides central electronic mailbox services to all University faculty, staff, and students. A person may choose to have his or her email delivered to an IT-managed mailbox or forwarded to another mail repository. Due to the confidential nature of some content transmitted via email, users handling such content are expected to use central services or forwarding to a departmental server within the Montclair State University address space.

3.2 Protection of Electronic Communications Services

Inbound Email
IT systems scan inbound email for content that may be characterized as spam. Where spam characteristics are found, the message may be tagged (through an update to the headers) or quarantined. IT also routinely scans all email for viruses and trojans. The scanning for viruses and trojans may also lead to a modification of the headers of the email, or further consequences, as explained below.

Because of the potentially harmful nature of the content of many messages or attachments, IT currently:

- Does not deliver messages containing attachments that have been identified as worms by our current anti-virus vendor;
- Deletes attachments that are identified as containing viruses by our current anti-virus vendor, and replaces them with a file called "deleted.txt";
- Blocks messages from external mailers that do not provide the proper identification per DNS. (Some spammers make use of improperly configured SMTP servers in an attempt to mask their true identity.)

IT reserves the right to block other incoming email that exhibits characteristics of spam, viruses, trojans, or other malware that could threaten the security or integrity of the campus network infrastructure or services.

Montclair State's email services also limit the size of inbound messages to 20 MB (including attachments.)

**Outbound Email**

- All outbound email must be routed through central IT mail relay services, or through an authorized departmental mail relay service.
- Messages up to 20 MB in size (including attachments) may be sent through Montclair State’s mail services.
- Outbound email will be scanned for viruses.

### 3.3 Misuse of Email

Montclair State email services may not be used to send unsolicited bulk or commercial email. They may not be used to send messages (such as large volumes of email messages or extremely large individual email messages) with the intent of disrupting a server or an individual's account on a server.

To protect the availability of the email service at Montclair State, users should refrain from sending chain letters, holiday cards or similar items to more than a few people. Unauthorized messages sent to large groups can impact central services in an adverse
manner. If a user has questions about whether or not to send a message to a large
distribution, that individual should check with a supervisor or contact the Montclair State
University Help Desk.

Forging, altering, or removing of electronic mail headers is also prohibited.
Violation of this or any other Montclair State University policy may result in disciplinary
action, up to and including suspension or termination.

3.4 Departmental Email Accounts (a.k.a “generic” accounts)

Departments that provide services in response to email requests should request the
creation of departmental email accounts (a.k.a. generic accounts) using the online
Generic Account Form located at https://netid.montclair.edu/GenericAccountCenter.

These generic departmental accounts will provide continuity as individual employees
move into and out of various departmental roles, ensuring that important email
requests for services will be appropriately directed to the person who can handle
the request. Privileges to access these shared email accounts will be managed by the
mailbox "owner", a department head or delegate.

4.0 Related Policies

Computing Account Management Policy
Password Management Policy