



User Account Retention Policy

NAME:	User Account Retention Policy
ISSUING DEPARTMENT	Campus Technologies
ISSUED DATE:	January 2003
REVIEWED DATE:	March 3, 2020
APPROVING AUTHORITY:	Cabinet
DATE REVISED:	January 27, 2020

INTRODUCTION

Email is the official means of communication between students, faculty and/or administration at Mansfield University. It is the expectation that all official communication will use the Mansfield University email address.

DEFINITIONS

Account

Refers to the actual user's credentials, username and password, that is used to access IT related resources.

Deactivated Account

Email, network drives and other stored data remain but the user is unable to access resources associated with their account and other IT related resources that belong to the University.

Purged Account

Permanent deletion of email, network drives and other stored data associated with a particular user account.

PURPOSE

The purpose of this policy is to define the length of time that user accounts and associated services will be maintained after the account holder leaves the university. It serves to maintain the security and efficiency of the university's network and resources.

POLICY

I. ACCOUNT CREATION

EMPLOYEES

New email accounts are created upon notification from Human Resources that a position has been accepted at the university and employment contract signed. All regular full-time, temporary full-time, regular part-time and some temporary part-time employees receive email accounts. The university may also provide accounts to auxiliary staff at its discretion.

Account addresses are created by using the first letter of the person's preferred first name and their last name. Their middle initial may be used to create a unique ID. Additionally, email "aliases" may be created later. However, the primary username will remain the same and still be used for login purposes. Any special characters such as hyphens are eliminated.

Cabinet reserves the right to provide provisional or early access to employee's account within 90 days prior to employee start date. The granting of provisional access is based upon the individual's contribution to the university's mission. Individuals needing early access should make their request to their supervisor. For approval, supervisors will forward these requests directly to a Cabinet member and communicate with Campus Technologies upon approval.

STUDENTS

All Mansfield University students receive an official Mansfield email account. Their Mansfield email account must be used for ALL Mansfield University electronic communications. New email account names are created within 24 hours of deposit, utilizing a student's last name, first letter of their preferred name, first letter of their middle name, and the day of their birth, with a maximum of 25 characters. In the event that this creation scheme results in duplicate Email addresses, additional letters of their middle name will be used. Any special characters such as hyphens are eliminated.

Faculty and administration will communicate academic and official information only to a student's Mansfield email account. Students are responsible for checking their account on a regular basis.

II. ACCOUNT TERMINATION

RETIRED FACULTY

All retired faculty are given the option of continued "Mansfield.edu" e-mail service for up to one year as they are considered for emeritus. Access to all university network resources including email, network drives and ancillary systems will be deactivated upon a year from their last work date, unless granted emeritus status.

EMERITI FACULTY

Emeriti faculty are given the option of continued "Mansfield.edu" e-mail service after retirement per the POLICY FOR RETIRED EMPLOYEES'/EMERITI FACULTY PRIVILEGES. Upon approval of this policy, emeritus faculty will have the privilege of a Mansfield email address provided they log into their account at least once a year. If their email account remains inactive (i.e. not logged into) for over a year, it will be considered abandoned and therefore deleted. Emeriti faculty who setup auto forwarding are still required to sign into their Mansfield accounts once a year to avoid account deletion.

RETIRED STAFF

It is the responsibility of retired staff to ensure they have copies of any personal data before their last date of service. Upon retirement, account will be deactivated and will no longer have access to all university network resources including email, network drives and ancillary systems.

SEPARATED EMPLOYEES

All separated, voluntary or otherwise, non-retiring employee email accounts are subject to closure without notice after the person's affiliation with the university is terminated. Since staff accounts are used for university business, access to those accounts may be restricted immediately upon termination. Cabinet reserves the right to allow continuance of individual accounts if doing so is demonstrably in the university's best interest.

GRADUATES

Graduating students will have access to their Mansfield email account after graduation. The address will change from @mansfield.edu to @mounties.mansfield.edu. Graduates will be notified via email when this change will occur. Alums will have the privilege of a Mountie email address provided they log into their account at least once a year. If their email account remains inactive (i.e. not logged into) for over a year, it will be considered abandoned and therefore deleted. Alums whom setup auto forwarding are still required to sign into their Mountie accounts once a year to preserve their email status.

NON-GRADUATING STUDENTS

The university reserves the right to suspend student email accounts at any time when a student withdraws (without exceptions), is dismissed or not returning to the university. Students who did not graduate and do not enroll or re-enroll, will still have access to their account for six months. It is the responsibility of the account holder to ensure they have copies of any desired data such as email, contacts, or user files before the end of this six-month period. After six months accounts will be deactivated.

ALL OTHER ACCOUNTS

All other accounts including but not limited to auxiliary employees, vendors, as well as community members are subject to closure without notice after the person's affiliation with the university is concluded. Since these accounts are used for university business, access to those accounts may be restricted immediately upon completion of service. Cabinet reserves the right to allow continuance of individual accounts if doing so is demonstrably in the university's best interest.

ACCOUNT RETENTION

All accounts are purged 180 days from the deactivation date unless the university has been notified of the need for preservation. This includes the account, email and network drive. Data and email cannot be recovered once an account is purged.

III. EMAIL OWNERSHIP AND PRIVACY

All communications and information transmitted, received, or archived in Mansfield University's email system belong to the university. Management has the right to access and disclose all email messages transmitted or received via the university's email system. Mansfield University may exercise its legal right to monitor email activity. Regarding email, employees and students should have no expectation of privacy. Be aware management may access and monitor email at any time, for any reason, with or without prior notice.

IV. EMAIL USAGE GUIDELINES

Email usage must conform to Mansfield University's Acceptable Use Policy. Exercise sound judgment and common sense when writing and sending email messages. When sending blind courtesy copies (BCC) and courtesy copies (CC), ensure the email does not violate another person's privacy by inadvertently sharing confidential information.

Individuals are responsible for managing their disk quota so that there is room for new mail. The university is not responsible for delivery problems caused by forwarding to non-official email accounts. Individuals should NEVER store passwords, account numbers or financial information as email records. Confidential or personal information such as Social Security Numbers should never be sent via an unencrypted email message.

V. EMAIL MISUSE AND ABUSE

Email messages should not be used to SPAM, threaten, harass or otherwise harm any individuals. If a user does receive an email that is menacing, offensive, and/or inappropriate, they must notify Campus Technologies about the message. Due to the nature of the message, HR or Campus Police may also need to be notified.

VI. EMAIL RETENTION AND BACKUP (FOR EMPLOYEES ONLY)

Mansfield University's email system is a delivery system for electronic communication. The automated system cannot discern differences between information of limited or transitory value and that of lasting value. Individual emails are not backed up or retained automatically. The email system, therefore, does not provide the functionality or the long-term storage capability required to maintain any official records of the university in individual email accounts.

All email messages with an ongoing legal, compliance, business, or project value (considered a "business record") must be retained in accordance with the university's Record Retention Policy. It is the responsibility of every email user to maintain their own emails. Since there is a limited amount of email storage in each user's email account, it is the user's responsibility to keep their email storage cleaned out and up to date.

Non-record email messages, including but not limited to administrative email (invitation to the university holiday party, meeting notices, etc.), do not need to be retained as a university record. Such messages only need to be kept if they are needed to conduct business. Failure to dispose of such messages wastes valuable university computer resources and employee time. However, if certain non-business records that need to be retained, they can be archived electronically. Please contact Campus Technologies for help on archiving email. All copies of non-record email (those with no ongoing legal, compliance, business, operational, project or historical value) can be deleted.

Mansfield University faculty, staff, and students should print copies or archive important documents and correspondence sent by email to be stored in relevant subject files or save the messages in a stable and retrievable electronic format on a long-term medium such as Flash Drives. Each individual, office, or department should have guidelines and retention plans that provide guidance to determine when documents and correspondence will be retained and for how long if they are official records for the university. Campus

Technologies should be contacted if certain business records must be retained for litigation reasons.

VII. PERSONAL USE OF EMAIL (FOR EMPLOYEES ONLY)

Mansfield University's electronic mail service is reserved primarily for university related communications. Employees may use their Mansfield email account for non-university related messages within the following guidelines:

1. Personal email should not interfere with the employees' work or other obligations and responsibilities to the university.
2. Personal email should not directly or indirectly interfere with the university's operation of computing facilities or electronic mail services or burden the university.
3. The use of Mansfield University's email system to solicit for any purpose, campaign for a political candidate, espouse political views, promote a religious cause, and/or advertise the sale of merchandise is strictly prohibited.
4. Personal Email usage must also conform to Mansfield University's Acceptable Use Policy.

VIII. SECURITY / ACCESS

Only authorized personnel are permitted to access other university email accounts without consent. Misuse of passwords, the sharing of passwords, and/or the unauthorized access of another user's account for any reason will result in disciplinary action.

IX. VIRUSES / SPAM

Be careful when opening email with attachments. While Mansfield University has SPAM and virus filters in place, there is the possibility that a malicious link or phishing attempt can bypass our system. If a user receives a strange message or unexpected email from someone, they should use caution and common sense before opening. When in doubt, contact the sender to verify the email is legitimate and safe. If an unknown file is accidentally opened or an unsafe link is clicked on, notify CT as soon as possible.

RESPONSIBILITY

It is the responsibility of the office of Campus Technologies to update and implement the policy, as needed.

DISTRIBUTION

This policy will be posted to the Policies and Procedures web page.