THE LEADER IN GLOBAL EDUCATION

FAIRLEIGH DICKINSON UNIVERSITY

Policy for Acceptable Use of E-Mail

Responsible Office:	University Systems and Security	Effective Date: 01/01/2018
Responsible Official:	Chief Information Security Officer	Last Revision:

TABLE OF CONTENTS

1.0 Introduction

The purpose of this policy is to ensure the proper use of e-mail by all those assigned a Fairleigh Dickinson University (FDU) e-mail account. This policy applies to any e-mail system that FDU has or may install in the future. It also applies to employee use of personal e-mail accounts via browsers, as directed below. All users of FDU e-mail systems have the responsibility to use their e-mail in an efficient, effective, ethical and lawful manner. E-mail users must follow the same code of conduct expected in any other form of written or face-to-face business communication. FDU may supplement or modify this policy for specific employees in certain roles. This policy complements similar FDU policies such as the Acceptable Use Policy and the Written Information Security Program (WISP) both of which can be found at http://isweb.fdu.edu.Please read and follow those policies as well.

The University subscribes to the 1940 Statement of Principles on Academic Freedom and Tenure and the 1940 and 1970 Interpretive Comments issued thereon, formulated jointly by the Association of American Colleges and the American Association of University Professors. Nothing in this policy is intended to supersede those statements and principles.

2.0 Ownership of Email Data

The University owns all University email accounts in the fdu.edu domain, or any subsequent domains it may create (University Email Accounts). Subject to underlying copyright and other intellectual property rights under applicable laws and University policies[1], the University also owns data transmitted or stored using the University Email Accounts.

3.0 Employee Responsibilities

FDU only supports the installation and usage of approved e-mail clients.

Usernames will be assigned as part of the University's e-mail registration process and reflect internally mandated e-mail naming conventions.

3.1 Acceptable Uses

- Communicating in a professional manner with other FDU associates about work-related matters.
- Communicating in a professional manner with parties outside FDU for business purposes.
- Personal communications that are brief and do not interfere with work responsibilities.
- Users are allowed to access personal e-mail accounts on a limited basis, without disrupting business responsibilities. Access can be gained only by using a browser. Use of e-mail-specific protocols, such as POP3 and IMAP4, is prohibited, since they require specific firewall ports to be open.
- Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.

[1] Links to the University's Intellectual Property policies appear at the end of this policy.

3.2 Unacceptable Uses

- Creating and exchanging messages that can be interpreted as harassing, obscene, racist, sexist, ageist, pornographic or threatening, as defined by University policies.
- Creating and exchanging information that is in violation of copyright or any other law. FDU is not responsible for an associate's use of e-mail that breaks laws.
- Personal communication that interferes with work responsibilities.
- Opening file attachments from an unknown or untrustworthy source, or with a suspicious or unexpected subject line.
- Sending unprotected healthcare data and personally identifiable consumer data or other confidential information to unauthorized people or in violation of FDU's Acceptable Use Policy, or the Written Information Security Program (WISP). , Health Insurance Portability and Accountability Act and/or Gramm–Leach–Bliley Act regulations. Exceptions may be authorized by the University Chief Information Security Officer working with the employee's supervisor. Communications that strain FDU's network or other systems unduly, such as sending large files to large distribution lists.
- Communications to distribution lists of only marginal interest to members, and replying to the entire distribution list when a personal reply is effective.
- Communications with non-specific subject lines, inarticulate language, and without clear purpose.
- Auto-forwarding e-mail messages from your University e-mail account.
- Using any e-mail system, other than FDU’s e-mail system, for FDU-related communications.
- Circulating chain letters and/or commercial offerings.
- Circulating unprotected healthcare data and personally identifiable consumer data that would violate U.S. Federal HIPAA and GLB regulations. Exceptions may be authorized by the employee's supervisor and in conjunction with use of a University-approved e-mail encryption service.
- Altering or forging the "From" line or any other attribution of origin contained in electronic mail or postings.
- Using any of the University systems for sending what is commonly referred to as "SPAM" mail (unsolicited bulk email)

4.0 Privacy Guidelines

The University typically does not review the content of electronic messages or other data, files, or records generated, stored, or maintained on its electronic information resources; however, it retains the right to inspect, review, or retain the content of such messages, data, files, and records at any time without prior notification. Any such action will be taken for reasons the University, within its discretion, deems to be legitimate. These legitimate reasons may include, but are not limited to,

- responding to lawful subpoenas or court orders;

- investigating misconduct (including research misconduct);
- determining compliance with University policies and the law; and
- locating electronic messages, data, files, or other records related to these purposes.

FDU maintains the right to monitor and review e-mail activity to ensure compliance with this policy, as well as to fulfill FDU's responsibilities under the laws and regulations of the jurisdictions in which it operates. Users should have no expectation of privacy.

- Except as otherwise stipulated in this policy, on termination or separation from FDU, FDU will immediately deny access to e-mail, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Except as otherwise stipulated in this policy, employees who leave FDU will have their mailbox deleted within six months of their termination date. The employee's manager may request that access be given to another employee who may remove any needed information within the same six month time frame.
- FDU reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received on the University e-mail system. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated FDU employees and/or designated external entities. Employees designated to review messages may include, but are not limited to, an employee's supervisor or manager and/or representatives from the HR, legal or compliance departments.
- FDU reserves the right to alter, modify, re-route or block the delivery of messages as appropriate. This includes but is not limited to:
  - Rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to FDU resources.
  - Rejecting or quarantining messages with suspicious content.
  - Rejecting or quarantining messages containing offensive language or topics.
  - Re-routing messages with suspicious content to designated FDU employees for manual review.
  - Appending legal disclaimers to messages.
- Electronic messages are legally discoverable and permissible as evidence in a court of law.
- Users of the University’s computing and electronic communications resources must understand that electronic messages, data, files, and other records generated, stored, or maintained on University electronic information resources may be electronically accessed, reconstructed, or retrieved by the University even after they have been deleted.

5.0 Security

As with any other type of software that runs over a network, e-mail users have the responsibility to follow sound security practices.

- Users should not use the e-mail system to transfer sensitive data, except in accordance with FDU data protection policies. Refer to the Written Information Security Program (WISP) found at http://isweb.fdu.edu under policies for more information. Sensitive data passed via e-mail over the Internet could be read by parties other than the intended recipients, particularly if it is clear text. Malicious third parties could potentially intercept and manipulate e-mail traffic.

- In an effort to combat propagation of e-mail viruses, certain attachment types may be stripped at the University e-mail gateway. Recipients will be notified via e-mail when this occurs. Should this create a business hardship, users should contact the University Technical Assistance Center (UTAC).

- Attachments can contain viruses and other malware. User should only open attachments from known and trusted correspondents. Suspicious attachments should be reported to the University Technical Assistance Center (UTAC).

- Spam is automatically filtered at the University gateway in a highly efficient manner. Errors, whereby legitimate e-mail can be filtered as spam, while rare, can occur. If business-related mail messages are not delivered, users should check their local spam folder or the daily spam digest. If the message is not there, users should contact University Technical Assistance Center (UTAC).

- Users will not be asked by OIRT or any other FDU group by e-mail for personal information such as usernames or passwords. Any such requests should not be responded to and should be referred to the University Technical Assistance Center (UTAC). Such approaches — known as phishing — are fraudulent approaches carried out for purpose of unlawful exploitation.

6.0 Operational Guidelines

FDU employs certain practices and procedures in order to maintain the health and efficiency of electronic messaging resources, to achieve FDU objectives and/or to meet various regulations. These practices and procedures are subject to change, as appropriate or required under the circumstances.

- For ongoing operations, audits, legal actions, or any other known purpose, FDU saves a copy of every e-mail message and attachment(s) to a secure location, where it can be protected and stored for three years. Recovery of messages from this store is prohibited for all but legal reasons.

- To deliver mail in a timely and efficient manner, message size must be less than 25MB. Messages larger than 25MB will be automatically blocked and users will be notified of non-delivery. Should this create a business hardship, users should contact the University Technical Assistance Center (UTAC).

Access to the content of electronic mail, data, files, or other records generated, stored, or maintained by any user may be requested from the University's Associate Vice President of Technology Infrastructure for the reasons set forth below and shall be authorized as follows:

(1) by the Associate Vice President of Human Resources for all University employees;

(2) by either Dean of Students for students; or

(3) by the General Counsel for the purposes of complying with legal process and requirements or to preserve user electronic information for possible subsequent access in accordance with this policy.

In all cases, the Office of the General Counsel must be consulted prior to making a decision on whether to grant access. In the case of a time-critical matter, if the authorizing official is unavailable for a timely response, the General Counsel may authorize access.

All full-time faculty who retire from the University may keep their email address for life if they request to do so.

All full-time faculty who leave the University for reasons other than termination for cause, may request email forwarding for up to six months.

7.0 Governance and Enforcement

This policy was created with input from the University's Data Security Incidence Response Team (DSIRT). At the request of the University's Chief Information Security Officer (CISO), the DSIRT will review this policy annually to ensure that FDU is in compliance with internal or external requirements. FDU faces liability if users violate the terms of this policy. Therefore, willful or repeated violations of this Acceptable Use Policy for e-mail can result in informal or formal warnings, the loss of e-mail privileges, and other sanctions including termination. Any such discipline shall be in accordance with processes and procedures of Human Resources and subject to any protections afforded under the University's agreement with "Office & Professional Employees International Union", the "Faculty Handbook", and similar documents. Third parties who violate this Policy may have their relationship with the University terminated and their access to campus restricted.

For assistance with this policy, please contact the University's Chief Information Security Officer (CISO).

Exceptions to this policy may be authorized by the University Chief Information Security Officer working with the employee's supervisor.

Policy violations should be reported immediately to the University's Associate Vice President of Technology Infrastructure

The University reserves the right to suspend an e-mail account while investigating a complaint or troubleshooting a system or network problem.

This document will be reviewed semi-annually and is available both electronically and in printed form at each of the Campus Computing Centers.

It is the user's responsibility to remain informed about the contents of this document.

OTHER RELATED AND APPLICABLE POLICIES

http://isweb.fdu.edu/policies/accept_policy.html

http://isweb.fdu.edu/policies/confidentiality_agreement_policy.htm

http://isweb.fdu.edu/policies/wisp_policy.html

http://view2.fdu.edu/legacy/privacylaws.pdf

http://view2.fdu.edu/academics/ctlt/policies/intellectual-property/

http://view2.fdu.edu/legacy/intellectualpropertystatementpolicyfinal.pdf