	Florida Gulf Coast University Policy Manual	**Policy: 3.021** **Approved:** 09/03/09
	TITLE: EMAIL POLICY	**Responsible Executive**: Vice President for Administrative Services and Finance **Responsible Office**: Office of Computing Services

POLICY STATEMENT:

Email communications are a vital way in which Florida Gulf Coast University employees conduct University business. It is the goal of the University to ensure email communications are being created, maintained and retained consistent with University policy and law.

REASON FOR POLICY:

The purpose of this policy is to notify employees that electronic communications are not private or confidential within the University and to educate employees on the appropriate and inappropriate use of electronic communications. This policy is also to provide information on the records retention requirements.

DEFINITION OF TERMS:

University Email:

Electronic communications that perpetuate University business, regardless of the computer or email account through which the email message is created.

Public Record:

All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. If the content of an email or its attachment meets this definition, it is a public record.

Transitory Messages:

Transitory Messages are messages with short-term value. Transitory messages are not intended to formalize or perpetuate knowledge, do not set policy or establish guidelines or procedures, certify a transaction or provide a receipt. Examples include emails reminding employees of a meeting or luncheon, certain phone messages. They are retained until obsolete, superseded, or their administrative value is lost.

PROCEDURES:

Access to employee emails

The email system is made available to University employees in order for them to conduct University business. As such, all email communications including those of a personal nature, are the property of the University, Consequently, this information may be accessed, copied, deleted or reviewed by the University at any time without the consent of the employee. Therefore, employees should understand they have no right to privacy as to any information or messages created received or maintained by Computing Services. Notwithstanding, individual privacy rights will be respected when the employee's activity neither interferes with job performance, is not illegal nor entails any risk of liability to the University. Incidental personal use of the employee's University email account is permitted, to the extent that it does not interfere with work duties. Moreover, other laws or University regulations may govern the content of emails (i.e. copy written documents, trade secrets, etc.).

Storage and retention public record

Email messages created in the course of University business may be subject to public records laws. Upon the expiration of the retention date of a public record, permission must be granted from the University's Records Manager Liaison Officer (RMLO) to destroy the record. Persons must contact the RMLO, complete the necessary form, and receive RMLO approval before deletion or destruction. The retention and destruction requirements apply to email messages and their attachments the same as any other public record document. The period of retention is based on the content of the message and attachment, not based on its format, i.e., electronic. Computing Services accepts no responsibility or liability for the storage and retention of individual email accounts, or any personal data stored on any University property.

Improper Use

The following are inappropriate uses of the University's email system. Items of this nature should not be sent. This list is not exhaustive, but contains key items that will be deemed inappropriate use of the email system and may be subject to disciplinary action including, but not limited to, termination of employment:

- Use of materials that contains explicit sexual content, are not necessary for University business (including academic instruction and research), and would be reasonably seen as obscene or pornographic.

- Use which is illegal, contrary to the University's best interest, or which violates or conflicts with the University's regulation and/or

policies on non-discrimination and anti-harassment.

- Uses designed to create revenue for the sender, not related to University business, for personal or pecuniary gain.
- Use of email, chat rooms or other Internet devices that is defamatory such as, but not limited to, racially or sexually charged messages, jokes or cartoons.
- Sending an email transmission whether inside or outside of the FGCU system such that it evokes others to transmit email messages which consequently bombard this University's or any other email system (i.e. bombardment).
- Use of Internet sites, which may damage or interfere with the University's computer network, including use that generates the delivery of "junk" electronic mail.
- Any actions that misrepresents the sender or attempts to mislead the recipient to the identity of the sender (i.e. false identification).
- Sending a letter generated in such a manner as to evoke the sending of an increasing number of email messages (i.e. chain letters).
- Messages intended to gather personal identification information ("Phishing").
- Virus hoaxes.
- Intentional messages sent that include or direct recipients to computer viruses, worms, or other harmful software.
- Political Activity. Activity of a partisan nature not related to the employee's authorized University duties and responsibilities.

Email security

Sharing of individual email accounts is prohibited. Those who share their account will be responsible for all activity from their account. Access to another user's email account must receive permission from the Vice President for Administrative Services and Finance as well as his or her Vice President or President's Direct Report.

Emails for University-wide distribution

Selected personnel have been approved to send All Staff, (A&P, SP), All University Faculty and Staff, and All Faculty email. Only those

persons having approval are authorized to send University-wide emails. Notwithstanding, in the case of critical system messages, a Vice President's or President's Direct Report approval is not required, but necessary approval may be attained at a lower supervisory level.

Closing of email accounts

Upon the separation of an employee, it is the supervisor's responsibility to ensure the separating employee's email account is properly retained consistent with the State of Florida's retention schedule. Email messages are retained for specific periods of time based on their content. With the assistance of Computing Services, supervisors may save the entire contents of the separating employee's account and later review the contents for proper disposition or retention. Separating employees' accounts will be deleted by Computing Services after 30 days following the separation.

Computer Crimes

Unauthorized use of University email can be a crime under the Florida Computer Crimes Act, the Computer Fraud and Abuse Act, as well as violate the laws of libel, privacy, copyright, trademark, obscenity, and child pornography. Employees must comply will all applicable laws or be in violation of this Policy.

Violations

Violations of this policy may result in disciplinary action consistent with University regulations, up to and including termination of employment.

HISTORY: New 01/30/06; Amended 09/03/09

APPENDICES: There are no appendices.

APPROVED 

President

September 3, 2009
Date