UNIVERSITY POLICY  IT-01.00-05/98

TO: The University of West Florida Community

FROM: Dr. Morris Marx, President

SUBJECT: Electronic Mail

Policy/Purpose: To articulate UWF policy concerning email

SECTION I: PURPOSE, SCOPE, RESPONSIBILITY, AND DEFINITIONS PURPOSE

Electronic mail, or ‘email,” a part of the campus life at the University of West Florida, offers tremendous opportunities for productivity enhancement and cost savings in the scholarly, service, and administrative operations of the University. However, it also provides the potential for misuse and abuse. Productive use of email, like any form of communication, requires understanding of common principles of style and etiquette, fair and responsible use, and consideration for the needs and rights of others.

Appropriate use of the University’s email systems should be the concern of every employee. In addition, Florida’s public records law offers many challenges to the use of email in the University setting, and exposes both the University and the employee to potential damage from the uninformed use of email. This document, therefore, seeks to: 1) educate all members of the University of West Florida community regarding the issues and practices of effective email use and 2) define University policy on the use and retention of electronic mail.

SCOPE

This policy concerns only electronic mail and its attachments. This policy pertains to all employees, volunteers, students, and other users of electronic mail affiliated through the University of West Florida (hereinafter referred to as “users”). The document covers email matters such as access, records retention, resources, public records, personal use, enforcement and sanctions and applicable federal and state statutes. A cyclical review of this policy has been incorporated to assess its effectiveness, efficiency and responsiveness to changes in information technologies and changes in email laws.

This document seeks to complement, not replace, existing University policies. Related University policies are outlined in Section IV. The final authority for records retention and disposition rules lies with the laws of the State of Florida and the officially-mandated practices governing Florida State Agencies. This policy seeks to interpret the implications of those laws and rules as they relate to electronic mail. It is not a replacement for them nor for the reader’s understanding of those more extensive regulations.
RESPONSIBILITY

The University’s Information Resource Manager (IRM) is responsible for the maintenance and publication of this policy and for periodic reviews to assess its continued effectiveness and viability. The IRM at the University of West Florida is the Chief Information Technology Officer. The current policy will be posted on the University’s various information servers, such as the UWF Web server, or may be requested from the IRM. The address of this web page is: http://nautical.uwf.edu/NAUTICAL/org.

The University assumes responsibility for the following:

A. To ensure that applicable laws, rules, regulations, and policies are followed.

B. To provide reasonable access to authorized users of the University’s email system.

C. To make available this policy to all users of the University’s email system.

D. To offer training sessions regarding the appropriate use of email and the information contained in this policy.

E. To terminate user accounts in a timely manner when the user’s affiliation with the University ceases, unless continued use is authorized by the Chief Information Technology Officer.

SECTION II: USE OF ELECTRONIC MAIL

Electronic mail is an official means of communication within the University of West Florida. UWF provides electronic mail services and facilities to the campus community for the furthering of the University mission, which includes the support of instruction, scholarly research and other creative activities, public service, and administrative activities of the University.

The University encourages the use of electronic mail as a convenient, timely, and cost-effective communications medium. The University also respects the privacy of the users of University electronic mail services. Those who use the University email services are expected to do so responsibly, that is, to comply with Florida and federal laws, with the policies and procedures of the University, and with normal standards of professional conduct and personal courtesy.

While it is impractical to completely delineate all approved and disallowed uses of the University email services, some encouraged uses of email and some prohibited uses are mentioned.

A. Permissible Uses of University Email Services

The following are examples of appropriate use of University electronic mail services.
a. The conducting of official University business, except in instances where use of email has been specifically discouraged.

b. Electronic dissemination of information, including the distribution of bulletins, memoranda, newsletters, reports, and committee communications.

c. Instructional use, specifically to enhance communications between students and instructors.

d. Facilitation of distance learning.

e. Support of research activities.

f. Electronic publications.

g. Service activities of faculty and staff.

h. Such uses as are consistent with the traditional academic freedom accorded to faculty members. See Section II. C. of this policy for personal use of email.

**B. Prohibited Uses of University Email Services**

The following uses of University electronic mail services are specifically prohibited.

1. University electronic mail services may not be used for:
   a. Violations of federal, state, and local laws, or of SUS or University policies and rules.
   b. Commercial purposes not under the auspices of the University.
   c. Personal financial gain (except as permitted under applicable policies).
   d. Constructing electronic communication so it appears to be from someone else.
   e. Obtaining access to the files or communications of others, unless expressly authorized to do so.

2. Electronic mail may not be used to represent, give opinions, or otherwise make statements on behalf of the University or any unit of the University unless the sender is authorized to do so by the University.

3. Email may not be used to interfere with the normal conduct of University business or the operation of University information technology services.

4. Email may not be used to transmit unsolicited material such as repetitive mass mailings, advertising, or chain messages.

5. Attempting unauthorized access to any portion of the email service or attempting to intercept any electronic communication transmission without proper authorization is prohibited.
6. Email should not be used in lieu of contracts or for formal agreements because of the ease of forgery or misrepresentation.

C. Personal Use

The University’s email system exists primarily to accomplish the work of the University; therefore, using it for personal communication should be done in a prudent and responsible manner. Furthermore, such use should not (1) directly or indirectly interfere with the University’s operation of computing facilities or electronic mail services; (2) burden the University with noticeable incremental costs; or (3) interfere with the email user’s employment or other obligations to the University. However, because of the difficulty of determining whether an email message pertains to University business or is a personal record, email users should be aware that an email message is a public record if it resides on University information technology facilities.

D. Encryption

This policy does not forbid the use of encryption by individuals; however, these individuals should recognize that the encrypted information, if determined to be a public record under the Florida Public Records Law, must be provided in accordance with the Florida sunshine law. Furthermore, under the Florida Public Records Law, if the information is in encrypted format, the requester must be provided with the software and key to read such data.

E. Use of Lists

Subscription to lists using the University’s email system is acceptable. If one subscribes, the subscriber must also make sure to know how to unsubscribe from the list, and do so when there is no longer a use for the information from the list. Users are cautioned that responding to email lists that may have hundreds of users could impact both the University email system and the email systems receiving the messages.

F. Email Etiquette

The use of email works best when everyone is considerate of others on the network. Therefore, email etiquette and appropriate techniques are described in Appendix B.

G. Interception and Retrieving of Messages

Users are not authorized to intercept or retrieve any email that is not sent to them unless expressly authorized to do so. An exception is the system’s personnel (i.e., a “postmaster”) who may need to see the mail when rerouting or disposing of undeliverable mail.
H. Cautions

Users of electronic mail should be aware of the following cautions.

1. Electronic mail may have been modified before forwarding.

2. Although electronic mail is often used in place of a phone call or voice mail message, it is closer in nature to a letter lacking both the visual and auditory content that comprises face-to-face communication. Thus, great care should be taken in crafting the “tone” of an email message, and in providing the recipient with the information needed to appropriately interpret the emotional nature of the contents.

3. University-provided electronic mail addresses and other Internet designations remain the property of the University. Such information constitutes directory information for students, faculty, and staff and may be disclosed or listed as directory information by the University. A student’s electronic mail address is considered directory information under the Family Educational Rights and Privacy Act (FERPA); however, it may be withheld upon the request of the student.

SECTION III: PRIVACY, REQUIRED ACCESS AND MONITORING

PRIVACY

Employees should have no expectation of privacy in email. The Attorney General has determined that email is a public record, Section AGO 96-34. Therefore, the privacy of email cannot be assured; it may be compromised by applicability of policy (including this policy) or law, by unintended redistribution, or inadequacy of current technologies to protect against unauthorized access. Extreme caution should be exercised when using email to communicate confidential or sensitive items. Therefore, a good rule of thumb regarding email messages is “not to put anything in an email message that you wouldn’t want posted on a bulletin board.”

Users should keep in mind that email messages can be easily printed, forwarded to others, or could even be delivered to the wrong address. Additionally, users of electronic mail services should be aware that although the sender and recipient have deleted their copies of an email record, backup copies may exist on the server or elsewhere.

Occasionally, network and computer personnel may, during the performance of their duties, inadvertently see the contents of an email message. They are not permitted to do so intentionally or disclose or otherwise use what they have seen. One exception is system’s personnel (i.e., a “postmaster”) who may need to see the mail when rerouting or disposing of undeliverable mail.

Chapter 119 of the Florida Statutes exempt certain categories of documents from disclosure
under the public records law, including but not limited to certain student records pursuant to Family Educational Rights and Privacy Act (FERPA) or potential trade secrets or patentable material relative to ongoing research at the University. Before any email is released pursuant to a public records request, any exempt information will be deleted from the email.

ACCESS

To further its mission, the University supports the sharing of information and the exchange of ideas. The University respects academic freedom, free speech, and privacy of information. As such, the University discourages the retrieval, inspection, monitoring, or disclosure of electronic mail messages without the prior consent of the user in possession of such messages except when: 1) required by and consistent with law, 2) there is a substantial reason to believe that violations of University policy or law have occurred, or 3) in exceptional cases, when required to meet time-dependent, critical operational needs determined by the Chief Information Technology Officer.

A. Consent

When appropriate, consent from the email holder should be sought by the University before any inspection, monitoring, or disclosure of University email records in the holder’s possession. Employees and students are, however, expected to comply with University requests for copies of email records in their possession that pertain to the University’s official business, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the University. Failure to comply can lead to disciplinary actions up to and including dismissal, the loss of information, systems usage privileges, and/or legal action.

B. Access Without Consent

When access is obtained without the holder’s consent, the following will apply:

1. Except in emergency situations, such actions must be authorized in advance and in writing by the authority specified by the law or policy under which the action is taken. If the authority is not specified, authorization must be sought from the appropriate University Vice President; this authority may not be further delegated downward. University counsel’s advice should normally be sought prior to authorization because of changing interpretation by the courts of laws affecting the privacy of electronic mail. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

2. In emergency situations (e.g., when the community or its members are endangered or when access to email records must be secured to ensure the preservation of evidence), the least perusal of the contents and the least action necessary to resolve the emergency may be taken immediately without authorization. However, the appropriate authorization must be sought without delay following the procedures of Section III above. If the action
taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

3. In either case, the responsible authorities or their designee should, at the earliest possible opportunity consistent with law and other University policy, notify the affected individual of the action(s) taken and the reasons for the action taken.

4. Actions taken in paragraphs one (1) and two (2) above shall be in full compliance with law or other applicable University policy. This has particular significance for email residing on computers not owned or housed by the University, and advice of university legal counsel must be sought prior to any action taken under such circumstances. Furthermore, this also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act [FERPA] of 1974, which applies equally to email as it does to paper records.

MONITORING

The University will not monitor electronic messages. However, the University, in the course of an investigation triggered by indications of misconduct, may examine email to insure that the laws and rules of the state and federal government are complied with. The University will respond to legal process and fulfill its obligations to third parties.

SECTION IV: RETENTION, DISPOSITION AND PUBLIC ACCESS RETENTION AND DISPOSITION

Retention schedules are based on a record’s informational content, not its format. Before deletion of an email message, the user must determine if the email is considered a “public record” (see Appendix A for definition). If the email is not a public record, it may be disposed of without consideration for retention and disposition requirements. Email that constitutes a public record must be disposed of in accordance with the records retention and disposition requirements and procedures provided in the University Records Management Manual. Users with questions regarding public records issues and record retention requirements should seek answers to these questions prior to deleting email messages.

Email is often used as a modern substitute for telephonic and printed communications, as well as a substitute for direct oral communications. The Florida Department of State has defined such messages as “transitory records” (see Appendix A). While these messages constitute public records, they are not required to be retained after the communication value is lost. They may be deleted at will without filing a records disposition notice, once the user determines that the communication value is obsolete, superseded, or administrative value is lost.

All other email which constitutes a “public record” (see Appendix A for definition) must be
retained for the required period of time according to University records retention schedules, and a records disposition notice must be filed with the UWF Records Management Department to initiate disposal.

While methods for reviewing, storing or deleting email vary, compliance with the retention requirements of the public records law can be achieved by doing one of the following:

1. Electronically store the public record email according to the conventions of your email system and retain it electronically pursuant to the University’s retention schedules. The technical details and methods of storing, retrieving and printing your email depends on the email system you use. Consult with your LAN administrator, or departmental computer support personnel, or the Information Resource Manager for details.

2. Print the email and store the hard copy in the relevant subject matter file, as you would any other hard-copy communication.

The user, and user department, has the responsibility for storage and retention of messages. Questions regarding storage and backups should be directed to the Information Resources Manager.

PUBLIC ACCESS

Access to public records, regardless of form, is required by law. The only exclusions are those public records specifically exempted by Florida statute (i.e., “limited access public records”, see Appendix A for definition).

Complete information and procedures regarding records retention, disposition and access is provided in the UWF Records Management Manual. Questions should be directed to the UWF Records Management Liaison Officer.

SECTION V: VIOLATIONS

Violations of any of the above guidelines are certainly unethical and may be violations of University policy or criminal offenses. Violations of this policy will be dealt with in the same manner as violations of other University policies, BOR rule, laws, or contracts, and may result in disciplinary review/action. In such cases, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the University, and legal action.

While it is impractical to delineate all violations in the use of the University email services, it is possible to identify some examples.
a. Minor violations: e.g., first offense for personal campaigning, solicitation, sending chain letters (congesting the email system), directly or indirectly interfering with the University’s operation of computing facilities or electronic mail services.

b. Major violations: e.g., violations of federal, state, or local laws, attempted security breaches, intercepting another’s email, constructing electronic communication so it appears to be from someone else, commercial use.

**Reporting Incidents**

For employees, such suspected violations shall be reported to the appropriate supervisor. For students, it will be the appropriate authority and Associate Vice President for Student Affairs. For serious violations and/or suspected breaking of the laws, these items should be reported by the supervisor immediately to the Chief Information Technology Officer and the Office of Human Resources Director (for employees) or Associate Vice President for Student Affairs (for students). For suspected violations by all other users, these items should be reported to the Chief Information Technology Officer.

**Sanctions**

Sanctions will be in compliance with the established disciplinary policies and procedures employed by the University. Grievances emanating from application of these policies and procedures will be processed using established policies and procedures. In the event of an investigation, files may be locked or copied to prevent destruction or loss of information.

**SECTION VI: RELATED LAWS, RULES, POLICIES, AND PROCEDURES**

UWF: UWF Computer Security Guidelines Florida Administrative Code, Sections 6C6-1.001 through 6C6-5.013 related to personnel issues
UWF Employee Handbook
UWF Presidential Memoranda dated April 6, 1995 “Policy Against Fraudulent or Other Wrongful Acts”
UWF Code of Student Conduct, Student Life Handbook

**Board of Regents: Computer Security Guidelines (Central Office Information Resource Management... revised March 1994)**

Chancellor’s Memorandum 94-12 “Policy Against Fraudulent or Other Wrongful Acts”
Florida Administrative Code, Sections 6C-5.900 through 6C-5.955 related to personnel issues

**State of Florida:** Florida Communications Fraud Act (8 17.034)
Florida Computer Crimes Act (815)
Florida Electronic Signature Act of 1996 (1.01)
Florida Public Records Law (119)
Federal:
1986 Electronic Communications Privacy Act (Title 18 Section 25101——Public Law 99-508)
1996 Telecommunications Act (Communications Decency Act) — Title V Section 501 ——
Public Law 104-104
1996 Electronic Freedom of Information Act (Title V, Section 552 et.seq.)
Electronic Records Management (Title 36, Chapter XII, Code of Federal Regulations, Part 1234)
Family Educational Rights and Privacy Act
Other: “The Bill of Rights and Responsibilities for Electronic Learners,” American Association
for Higher Education

SECTION VII: REFERENCES

Harris, D. “Electronic Mail Etiquette”
Pierce, T. “Business Netiquette Internationa,”
Sherwood, Kaitlin Duck, “A Beginner’s Guide to Effective Email,”
“Bill of Rights and Responsibilities for Electronic Community of Leaders,” American
Association of Higher Education.
“Bill of Rights and Responsibilities for the Electronic Community of Learners,” American
Association of Higher Education.
Electronic Frontier Foundation

SCHOOLS:

Baylor University
University of California
University of Chicago
Cornell University
University of Delaware
Florida International University
University of Florida
University of Illinois
Kent State University
University of Michigan
Stanford University

APPENDIX A

Definitions

Electronic Mail
Electronic mail includes electronic transfer of information (whether messages, memoranda, and
other written documents) from a sending party to one or more receiving parties via an
intermediate telecommunications system.
Electronic mail (or email) can refer to the electronic mail service or to an individual electronic mail message.

**Electronic Records**
Electronic records are records in electronic form, including numeric, graphic, and textual information, that may be recorded in any machine-readable media form. Electronic records can include, but is not limited to, magnetic media such as tapes, disks (hard disks, floppy disks, optical disks), compact disks, and similar media used to store information electronically including computer systems and servers. Electronic records encompass electronic mail as a type of electronic record.

**Limited Access Public Records**
Limited access public records are those records which the Florida Legislature has expressly authorized by statute to be closed from public inspection. These exemptions from the Florida Public Records Law are specifically defined by law and only apply to a very small percentage of public records. Unless a specific statutory exemption can be cited, all official agency records of the University of West Florida should be considered public records and open to public inspection.

**Official University Business**
Official University business includes any activities of employees, agencies, and departments of the University of West Florida performed pursuant to the mission of the University. These have been defined by the courts as including any activity involving the expenditure of public funds, decision-making, and policy development.

**Personal Records**
Personal records are records of individuals, including electronic records and electronic mail which do not fall under official University business. Personal does not mean the individual but rather the nature of the record.

**Public Records**
Public records include all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material regardless of physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business of any agency. [Ch. 119.01, amended July 1, 1995 Florida Statutes]. The Florida Supreme Court has further interpreted this law to cover any material prepared in connection with official agency business which is intended to perpetuate, communicate, or formalize knowledge of some type including all of the information stored on a computer. By law, all records--electronic or not--of the University of West Florida (its officers, employees, departments, and agencies) are deemed public records if they are made or received as part of the official business of the agency.

**Transitory Records**
Transitory Records are those which do not set policy, establish guidelines or procedures, certify a
transaction, or become a receipt. Such records are created to communicate information rather than serve to perpetuate knowledge. Some electronic mail can be considered transitory records especially those which tend to be informal and similar to communication that might take place during a telephone conversation or hallway discussion. Other examples of transitory records would include but not be limited to voice mail, self-sticking notes, telephone messages, and messages with short-lived, or no administrative value.

APPENDIX B

Email Etiquette

Introduction
The first rule of etiquette is to have and show consideration to others. You should consider how the other party is going to receive and interpret your message, thereby preventing misunderstandings.

Email Communication
Communication via email can be seen in two ways:

• No different from writing on UWF’s letterhead, as a business communication. This requires a certain degree of formality.
• Because of its speed and broadcasting ability, as something fundamentally different from paper-based communication. Given its fast turnaround time, it is more conversational than traditional media, and therefore it’s not necessary to make everything completely clear and unambiguous, because the recipient can ask for clarification. Email can thus be much sloppier and less formal.

The truth is somewhere in between. Email can be used for both formal business communication and for informal, conversation-like exchanges.

Subject Line
Use a subject line that clearly reflects the content of the email message. It should be brief (many email programs truncate long subject lines), does not need to be a complete sentence, and should place the recipient on the right context to read your message. Email programs usually preface the subject line with Re: or RE: (for Regarding) when you are responding to a mail message. Prepending the subject of your message with information regarding the required response is useful. For example, prefacing the subject line of an informational message with FYI (For Your Information) as in: Subject: FYI: Power shutdown Friday afternoon
Using URGENT: will call the attention of the recipient, especially if you know he/she gets a lot of email.
The Message
Construct your message as a series of short paragraphs so it will be easier to read on a computer screen. In general, email messages are much shorter than written memoranda. If your message is more than a page long, send it as an attachment.

Keep email messages focused on one subject. This will help keeping your messages short. When replying, refer to the text of the original message by keeping enough lines to provide context. Keep the thread by responding in-between the incoming message’s text. As a general rule, more than half the lines in message should be yours. If you have to include the whole message that you are replying to, include it at the end of your response.

It is often recommended to keep email messages terse. However, don’t try too hard to be brief, to the point of not communicating. An extremely brief response to a message without the original message as a reference may be completely out of context and not understood.

It is much too common to respond to messages in anger, only to regret it later. The speed by which one can respond to a message takes away from the needed time to think things over. When angry, wait a while before responding, don’t react immediately.

Don’t use smileys (:-) :/- etc.) for formal communications. These are fine for personal notes but are quite inappropriate for business use.

Personal Name and Email Addresses
Email programs allow you to define your full name and attach it as part of your messages. Make sure you do so. If in doubt, send yourself a mail message and test whether the recipient would be able to determine who sent it.

Signature
Signatures should be informative but brief. Most email programs allow you to define your signature and attach it automatically at the bottom of all your messages. This is very handy, especially when communicating with people who may not know you personally. Keep it short and concise: it should include your name, position, affiliation and Internet address and should not exceed more than 4 lines. Optional information could include your address and phone, and fax number.

Capital Letters
Capital letters ARE INTERPRETED AS SHOUTING. Unfortunately, their use is a legacy from old mainframe systems that could not handle upper cases. Avoid using them.

User Responsibilities
People expect responses to their email. It is the user’s responsibility to administer their mailbox,
including:

- Check your email at least daily.
- Respond to your email promptly.
- Message deletion should follow the same guidelines used for disposal of any other document.
- Never assume that your email, especially if going outside the UWF campus, can be read by no one except yourself and the person to whom you are sending the email.
- Follow chain of command procedures for corresponding with superiors. For example, don’t send a complaint via email directly to the top just because you can.

References
Harris, D. “Electronic Mail Etiquette”.
Pierce, F. “Business Netiquette International”.
Shwerwood, Kaitlin Duck, “A Beginner’s Guide to Effective Email”.

The Ten Commandments for Computer Ethics

- You shall not use a computer to harm other people.
- You shall not interfere with other people’s computer work.
- You shall not snoop around in other people’s files.
- You shall not use a computer to steal.
- You shall not use a computer to bear false witness.
- You shall not use or copy software for which you have not paid.
- You shall not use other people’s computer resources without authorization.
- You shall not appropriate other people’s intellectual output.
- You shall think about the social consequences of the program you write.
- You shall use a computer in ways that show consideration and respect.

APPENDIX C

Frequently Asked Questions (FAQs)

Q: Is my email private?
A: Email created or received by the University of West Florida employees concerning official business is subject to the public records law and open for inspection. Users should not have an expectation of privacy in email. Users should exercise extreme caution in using email to communicate confidential or sensitive matters.

Q: Is there monitoring or inspection of email by staff? If so, under what circumstances?
A: The University will not monitor electronic messages in a routine manner. (See Section III, “Monitoring” of this policy for a list of the circumstances under which you email could be
What “privacy” should individuals expect using university systems?
A: Occasionally, network and computer personnel may, during the performance of their duties, see the contents of an email message. They are not permitted to do so intentionally or disclose or otherwise use whatever they have seen. One exception is system’s personnel (i.e., a “Postmaster”) who may need to see the mail when rerouting or disposing of undeliverable mail. If privacy is needed for sensitive material, you may obtain a personal encryption program which encodes the messages before it leaves your computer, so intermediate operators can not inadvertently read your message. The recipient must have the same program and your personal encoding keys to decode the messages at the other end. The University can use legal process to obtain these privacy keys if they are needed for valid investigations.

Are there situations where the security of individual email accounts may be compromised WITH authorization?
A: Yes, since the University resources are being used to create and store files, users should understand that the University must assign certain individuals responsibility for maintaining, repairing, and further developing those resources. In the normal course of doing their assigned work, some individuals, by virtue of their specific responsibilities (e.g., a “postmaster”), may have special access privileges and therefore to the content that resides in those resources. [See Section III, “Privacy”.

May I give my password to someone else to use?
A: It is not a recommended practice to give out your password and User ID to another party since it can cause problems. The University will hold you personally responsible for any misuse of your email account.

Once I receive an email message from someone, is it OK for me to forward it to whomever I choose?
A: Yes, unless the message contains specific copyright information or the sender has requested you treat the message in a confidential manner.

How do I remove my name from mass distribution lists on campus? (Someone puts an individual on a distribution list (e.g., “all faculty”) and the recipient doesn’t want to be a part of the distribution list...how to handle this situation.)
A: Send a message to whomever is handling the list and ask them to remove you from it.

Is it acceptable for me to use the University’s email system for personal communications?
A: Yes, when such use does not interfere with a University function [Also see Section II.C.]

How can I tell if my email is being received by the addressee? (notification to sender of undeliverable mail)
A: Some emailer systems have an acknowledge function to let you know when a message has been received. If you sent your message to a bad address, your server should send your message back saying that it is undeliverable.
Q: Are email addresses published? If so, where can I find them?
A: Yes, such information constitutes directory information regarding students, faculty, and staff. The University-supplied electronic mail addresses of employees maybe disclosed or listed as directory information by the University. A student’s electronic mail address is considered a student record and included in the FERPA definition of directory information, however, the electronic mail addresses of students may be withheld upon the request of the student. Email addresses for staff members are published in the campus telephone directory.

University of West Florida
Email Policy Task Force
Last Updated: May 21, 1998

Last printed 06/03/02 2:24 PM

Approved:  

Date:  5/98