

# **ELECTRONIC MAIL GUIDELINES**

**April 18, 2000**

# TABLE OF CONTENTS

I.	SPECIFIC USE PROVISIONS	
A.	Provision of Service .....	1
B.	University Property .....	1
C.	Authorized Service Restrictions .....	1
D.	Authorized Access and Disclosure .....	1
E.	Indemnification of the University .....	2
II.	MISUSE	
A.	Illegal Use .....	2
B.	Failure to Follow Law .....	2
C.	Prohibited Use .....	3
D.	Sending Unwanted Mail .....	3
E.	Commercial Activities .....	3
F.	False Representation .....	3
G.	Straining Computer Facilities .....	3
III.	PERSONAL USE .....	4
IV.	CONFIDENTIALITY .....	4
A.	Laws and Policies .....	4
B.	Access .....	4
C.	Electronic Mail Directory .....	4
V.	SECURITY AND PRESERVATION	
A.	Professionalism .....	4
B.	Hardware and Software Capabilities .....	5
C.	ID's and Passwords .....	5
D.	Standards, Measures, and Procedures .....	5
VI.	VIOLATIONS .....	6
VII.	ONLINE POLICIES, GUIDELINES, & PROCEDURES .....	6

## I. SPECIFIC USE PROVISIONS

- A. Provision of Service: Electronic mail services may be provided by University organizational units in support of the University's mission.
- B. University Property: Electronic mail services are extended for the sole use of University faculty, staff, students and other appropriately authorized users to accomplish tasks related to and consistent with the University's mission. University electronic mail systems and services are University facilities, resources, and property as those terms are used in University policies and applicable law. Any electronic mail address or account assigned by the University to individuals, sub-units, or functions of the University, is the property of the University.
- C. Authorized Service Restrictions:
1. Electronic mail users are required to comply with state and federal law, University policies, and normal standards of professional and personal courtesy and conduct. Access to University electronic mail services is a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the electronic mail user when:
    - required by and consistent with applicable law or policy,
    - there is a reasonable suspicion that violations of policy or law have occurred or may occur; or
    - required to meet time-dependent, critical operational needs.Such access restrictions are subject to the approval of the appropriate University supervisory or management authority (e.g., department heads, systems managers, etc.). The autonomous operational units of the University should establish or identify these authority levels.
  2. University operational units may define additional "Conditions of Appropriate Use" for local computing and network facilities to supplement these Guidelines with additional detail, guidelines, or restrictions. Such Conditions must be consistent with and subordinate to these Guidelines, and are intended to deal primarily with situations of limited resource supply.
  3. When an individual's affiliation with the University ends, the University may attempt to redirect electronic mail for a reasonable period of time as determined by the University for purposes consistent with this Guideline and the University's mission. The University may elect to terminate the individual's electronic mail account or continue the account, subject to approval by appropriate University supervisory and systems operational authority.
  4. Additional space management procedures will be implemented as necessary. Example: When disk space is limited, large electronic mail files (generally 500,000 bytes or larger) may be deleted to preserve the integrity of the system. At such times, the user will have the option of restoring select files upon request.
- D. Authorized Access and Disclosure:
1. The University may permit the inspection, monitoring, or disclosure of electronic mail when:

- a. Required by or consistent with applicable law or policy such as the Family Educational Rights and Privacy Act (regarding access to student records), or any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on University systems to be accessed by authorized personnel in certain circumstances;
  - b. There is a reasonable suspicion that violations of law or University policy have occurred or may occur; or
  - c. There are time-dependent, critical operational needs of University business if the University determines that the information sought is not more readily available by other means.
2. In such instances, the University will, as a courtesy, normally try to inform electronic mail users prior to any inspection, monitoring, or disclosure of electronic mail records, except when such notification would be detrimental to an investigation of possible violation of law or University policy. Users are required to comply with University requests for access to and copies of electronic mail records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate University personnel policies.

E. Indemnification of the University: Users agree by virtue of access to the University's computing and electronic mail systems, to indemnify, defend and hold harmless the University for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of University electronic mail and computing systems, services, and facilities except where the claimed activity or lack of activity is behavior for which the University provides representation and indemnification as provided in appropriate University Policies.

## II. MISUSE

- A. Illegal Use: Using electronic mail for illegal activities is strictly prohibited. Illegal use may include, but is not limited to: obscenity; child pornography; threats; harassment; theft; attempting or accomplishing unauthorized access to data or attempting or accomplishing to breach any security measures on any electronic communications system; attempting or accomplishing to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark, or defamation law.
- B. Failure to Follow Law: Failure to follow state law with regard to the disposition of electronic mail records may lead to criminal charges.

- C. Prohibited Use: In addition to illegal activities, the following electronic mail practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this policy; altering electronic mail system software or hardware configurations; or interfering with the work of others or with the University or other computing facilities.
- D. Sending Unwanted Mail: If a user has been requested by another user via electronic mail or in writing to refrain from sending electronic mail messages, the recipient is prohibited from sending that user any further electronic mail messages until such time as he/she has been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of these Guidelines.
- E. Commercial Activities: University electronic mail services may not be used for: commercial activities not approved by appropriate supervisory University personnel consistent with applicable policy; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section I and III of these guidelines; uses that violate other University policies or guidelines; or uses inconsistent with applicable state or federal law. Applicable University policies include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or regarding sexual or other forms of harassment. Use of electronic mail-user identifications for commercial purposes is prohibited.
- F. False Representation: Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of Ferris State University."
- G. Straining Computer Facilities: University electronic mail services shall not be used for purposes that could reasonably be expected to cause, directly, or indirectly, strain on any computing facilities, or interference with others' use of electronic mail or electronic mail systems. Such uses include, but are not limited to, the use of electronic mail services to:
- Send or forward chain letters.
  - "Spam," that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.
  - "Letter-bomb," that is, to resend the same electronic mail repeatedly to one or more recipients.

### III. PERSONAL USE

University electronic mail services may be used for incidental personal purposes provided that such use does not:

- Directly or indirectly interfere with the University operation of computing facilities or electronic mail services.
- Interfere with the electronic mail user's employment or other obligations to the University.
- Violate these Guidelines, or any applicable policy or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation, copyright violation or illegal activities.

Electronic mail messages arising from such personal use shall, however, be subject to access consistent with these Guidelines or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

### IV. CONFIDENTIALITY

- A. Laws and Policies: The confidentiality of electronic mail cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including these Guidelines, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using electronic mail to communicate confidential or sensitive matters, and should not assume that their electronic mail is private or confidential. Use does not carry with it a reasonable expectation of privacy.
- B. Access: Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, whether the information is maintained on paper or whether it is found in electronic mail or other electronic records.
- C. Electronic Mail Directory: The University may elect to publish student electronic mail addresses as directory information, consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). Individual students may, consistent with University policy and FERPA, request that the University not treat the address as directory information. Requests for identification or release of a student's electronic mail address should be directed to the Office of the Registrar.

### V. SECURITY AND PRESERVATION

- A. Professionalism: Electronic mail users and operators must follow reasonable professional practices in providing for the security of electronic mail records, data, applications programs, and systems programs under their jurisdiction.

- B. Hardware and Software Capabilities: Users and operators must guard against storage media deterioration and electronic mail record inaccessibility due to hardware or software obsolescence. To eliminate these situations, users must make provision for future accessibility by:
- Migrating all official electronic mail records to the next generation of hardware or software; or
  - Migrating only current official electronic mail records to new hardware or software, or converting official electronic mail records not migrated to other media (e.g., optical disk, COM) for short-term storage or to "eye-readable form" (i.e., paper or microfilm) for long-term storage and preservation.
- C. ID's and Passwords: Users are responsible for safeguarding their identification (ID) codes (also known as login name) and passwords, and for using them only as authorized. Each user is responsible for all electronic mail transactions made under the authorization of his or her ID, and for all network electronic mail activity originating from his or her data jack. Use of electronic mail-user identifications for commercial purposes is prohibited. Access to user identifications or information may not be loaned or sold.

You should be aware that although service providers provide and preserve security of files, account numbers, ID codes, and passwords, security could be breached through actions or causes beyond their reasonable control. You are urged, therefore, to choose your passwords wisely and to **change them periodically**; and to follow the security policies and procedures established to control access to and use of administrative data.

To ensure that every customer has a unique ID code, all user ID's will be created in a central database that is maintained by IS&T. Before a new account is created on a file server, the correct database must be consulted. Every customer will have one unique ID on campus, and use the ID for non-mainframe services. Using the first seven (7) characters of the users last name, and the first character of the first name will form the user's ID code. This will comprise no more than eight characters. If following this convention does not total eight (8) characters, the ID will not be padded to make up characters.

- D. Standards, Measures, and Procedures: Each operational unit should establish:
- Standards for official electronic mail records identification and file organization.
  - Measures for protecting sensitive official electronic mail stored electronically.
  - Procedures for file back up.

## **VI. VIOLATIONS**

Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. The appropriate University authorities and/or law enforcement agencies will process violations. Violations may result in revocation of electronic mail service privileges; academic dishonesty; faculty, staff or student disciplinary action up to and including termination of employment; referral to law enforcement agencies; or other legal action.

## **VII. ONLINE POLICIES, GUIDELINES, AND PROCEDURES**

Users of this document are encouraged to refer to online versions of this and other University documents on the University's homepage on the World Wide Web.

Adopted, with permission from the University of Arizona