TITLE: Appropriate Use of Electronic Communication and Information Network Resources

ORIGINATOR: Director of Information Technology Services

APPROVAL DATE: February 8, 2010

EFFECTIVE DATE: February 8, 2010

PURPOSE: This policy outlines the application of the principles that govern our academic community in the appropriate use of electronic communications and information network resources.

REVIEWER: Administrative Council

REVIEW DATE: November 2014 and every 5 years thereafter

OPERATING DETAILS:

Official Communications

Students, faculty, staff and administration at Mississippi University for Women increasingly rely on electronic communication, motivated by its convenience, speed, cost-effectiveness, and environmental advantages. Because of its general acceptance, use**,** and availability, the University considers email to be one of the official means of communication within the MUW community. Accordingly, the University will use the MUW assigned student, faculty and staff email as the primary address for purposes of official communications with the full expectation that these emails will be received and read in a timely fashion. Students, faculty and staff should check their email frequently and consistently, with the recognition that certain communications may be time-critical.

The University ITS Department issues email accounts to all MUW students, faculty and staff. MUW email users can elect, at their own risk, to have their university email automatically forwarded to an outside account. The University is not responsible for the handling of email by outside vendors, nor are individuals who use outside accounts absolved from responsibility for messages not received or read. If a full inbox or the unmonitored use of a “spam” filter causes undeliverable messages to be returned, these messages will be considered delivered and further action will not be required of the University.

Electronic Communications Privacy and Confidentiality

The Mississippi University for Women will make reasonable effort to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of an individual user's use of the University's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored.

Electronic Communications Authorized Users

Only University faculty, staff, students, and other persons who have received permission under the appropriate University authority are authorized users of the University's electronic mail systems and resources.

Electronic Communications Prohibited Uses

a. Personal use that creates a direct cost for the University is prohibited.
b. Personal monetary gain or commercial purposes that are not directly related to University business.
c. Sending copies of documents or inclusion of the work of others into electronic mail communications in violation of copyright laws.
d. Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems.
e. Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business.
f. Use of electronic mail systems for any purpose restricted or prohibited by State or Federal laws or regulations.
g. "Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else.
h. "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.
i. Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

University Access and Disclosure of Electronic Communications

1. General Provisions

    a. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty’s, staff’s, students', and other users' electronic mail without the consent of the user. The University will do so

when it believes it has a legitimate business need including, but not limited to, those listed in paragraph 3 (below), and only after explicit authorization is obtained from the appropriate University authority.

b. Faculty, staff, and other non-student users are advised that the University's electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.
c. Confidentiality of student records is protected under FERPA (Family Education Rights and Privacy Act). All use of email, including use for sensitive or confidential information, will be consistent with FERPA.
d. Any user of the University's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate University authority.

2. Monitoring of Communications

   The University will not monitor electronic mail as a routine matter**,** but it may do so to the extent permitted by law as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems.

3. Inspection and Disclosure of Communications

   The University reserves the right to inspect and disclose the contents of electronic mail:

   - in the course of an investigation triggered by indications of misconduct or misuse,
   - as needed to protect health and safety,
   - as needed to prevent interference with the academic mission, or
   - as needed to locate substantive information required for University business that is not more readily available by some other means.

   The University will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the University's obligations to third parties.

4. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

The contents of electronic mail communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

5. Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications

   Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must submit a written request to the University's President. The request should be as specific as possible as to what information is being sought, with whom this information could be shared, and the expected duration of the access.

Information Network Resources

All users are expected to utilize University information network resources in a responsible manner. You are expected to take reasonable measures to ensure that traffic entering the MUW network from other networks conforms to this policy. Conversely, you are expected to take similar measures to avoid situations where traffic from the MUW network violates the policies of connecting networks. The unauthorized use of resources is prohibited and, in many cases, may be violations of the law. We are guided by the law in noting that unauthorized use includes, but is not limited to the following types of activities.

Harassment or threats to specific individuals, or a class of individuals:

- Transmitting unsolicited information that contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct.
- Using e-mail or newsgroups to threaten or stalk someone.
- Transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination.

Interference or impairment to the activities of others:

- Creating, modifying, executing or retransmitting any computer program or instructions intended to: (1) obscure the true identity of the sender; (2) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the

permission of the owner; or (3) examine or collect data from the network (e.g., a "network sniffer" program).

- Authorizing another person or organization to use your computer accounts or MUW network resources. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not share your password with anyone else or provide access to MUW network resources to unauthorized persons.
- Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

Unauthorized access and use of the resources of others:

- Use of University resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.
- Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).
- Making unauthorized copies of copyrighted materials. You should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.

Damage or impairment of University resources:

- Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program), (2) damaging or violating the privacy of information not belonging to you, or (3) misusing or allowing misuse of system resources.
- Use of University resources for non-University related activities that unduly increase network load (e.g., chain mail, network games and spamming).

Unauthorized commercial or political activities:

- Using University resources for one's own commercial gain, or for other commercial purposes not officially approved by the University, including web ads.
- Using University resources to operate or support a non-University related business.
- Use of University resources in a manner inconsistent with the University's contractual obligations to suppliers of those resources or with any published University policy.
- Use of University resources for partisan political activities.

Violation of city, state or federal laws:

- Pirating software, music and images.
- Effecting or receiving unauthorized electronic transfer of funds.
- Disseminating child pornography or other obscene material.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

When Inappropriate Use of Network Resources Occurs

While the University desires to maintain user privacy and to avoid the unnecessary interruption of user activities, the University reserves the right to investigate unauthorized or improper use of University resources, which may include the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to University policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user privileges, deletion of files, and disconnection from the MUW network, referral to student or employee disciplinary processes, and cooperating with the appropriate law enforcement officials and government agencies.

The University is not responsible for information, including photographic images and musical recordings, published on or accessible through personal web pages, including personal home pages. The University does not monitor the contents of these personal web pages. The individual or group creating or maintaining personal web pages is solely responsible for the content of the web page and may be held civilly and criminally liable for the materials posted on the web site.

Questions Relating to This Policy

The examples of unauthorized use set forth above are not meant to be exhaustive. Questions about this policy or of the applicability of this policy to a particular situation should be referred to admin@muw.edu or the Director of Information Technology Services.