

Electronic Messaging Guidelines

Contents

I.	Introduction	1
II.	Electronic Messaging Principles	1
A.	Shared Resource:	1
B.	Technical constraints:	2
C.	Privacy:	2
D.	Transportation versus storage:	2
E.	Global Connectivity:	2
F.	Cost:	2
G.	Message Content:	2
III.	Never share your university messaging credentials with others	3
A.	Working with Mobile Devices	3

I. Introduction

These guidelines explain principles and expectations that govern individual and common use of JMU's electronic messaging systems. Questions or comments about the Electronic Messaging Policy or these Guidelines should be directed to it@jmu.edu.

II. Electronic Messaging Principles

A. Shared Resource:

Messaging systems use many network and computing resources that are shared by the campus community as well as services shared by the world. The individual services, collectively referred to as electronic messaging, each evolved to address a particular need and are designed to make efficient use of resources in a given situation. Therefore, messages should be sent using the technology appropriate to the task and in keeping with university policies regarding appropriate use (see university Policy 1207). Some typical guidelines for various services include:

- E-mail and instant messaging: person-to-person
- E-mail list: small group discussions
- List, forum, chat services: large group discussions
- Web site: information distribution

B. Technical constraints:

Messages are sent through electronic messaging systems using store and forward technology. This means that the messages typically pass through multiple systems, some of which may not be fully secure or reliable.

C. Privacy:

While privacy cannot be assured on all systems in a particular message route, Information Technology will work to assure system security and availability on the computer systems it administers. Additionally, IT personnel who carry advanced privileges will not read private messages except as required in pursuit of security or system management anomalies and will do so under the direction of IT management. Recipients of electronic messages must also be aware that the identity of the sender may/may not be authentic. Even though the identity of the message sender is not authenticated by many current messaging systems, forgeries are nonetheless unacceptable. Also, senders must be aware that delivery of a message cannot be fully assured. As with paper mail, a return receipt or response from the recipient is the only reliable way to determine that a message has been read.

D. Transportation versus storage:

While there is a limited amount of storage space for new/incoming messages contained in the messaging systems, it is not to be used for long-term storage or archive. Instead, electronic messaging systems are to be considered a transportation mechanism. As with any transportation mechanism, the related issues of system failure and recovery should be considered. While IT will perform periodic backups of messages in transit, these should be viewed as insurance against system failure, not as a mechanism to restore individual messages. Local backups of message originals should be made for any critical communications. Individuals are responsible for the long-term storage of electronic messages ensuring that they reside in areas that are adequately protected.

E. Global Connectivity:

Connection to global networks such as the Internet and use of services like forums, chat rooms, instant messaging, etc. pose additional challenges. Each network, mailing list and news group has its own policies, procedures and rules of conduct. As a member-owner of these services, the university will act as necessary to protect its shared interest and as a condition of continued use of global resources. This does not, however, mitigate the individual's responsibility within this environment.

F. Cost:

The costs associated with electronic messages are unlike those for traditional paper-based mail. The cost of electronic messages is born primarily by the recipient(s), not the sender. Therefore, no junk mail/SPAM shall be sent using university messaging systems. Specific examples of junk/SPAM mail are: chain letters, advertisements and other unsolicited mass mailings as well as excessive or inappropriate postings to news groups.

G. Message Content:

The content of any message sent through the messaging system is the sole responsibility of the individual sending the message. Harassment, obscenity, forgery and other illegal forms of expression are not acceptable use of university resources. The only enforceable restrictions on content of electronic messages are those that apply generally to verbal or written communication (slander, harassment, SPAM, etc.). When such restrictions need to be enforced, the same administrative, judicial and criminal processes as for non-

computer communication may be invoked. Use of electronic messaging systems does not change what is and is not an illegal communication.

The university will not censor or regulate messages based on content or views expressed by the sender or implied by the receipt. Individuals who use resources such as forums/newsgroups, e-mail lists, chat services, etc. shall decide for themselves whether the forum and content are appropriate to their needs. The university will treat these services as an educational resource. Transmission of information by electronic means does not negate intellectual property rights, copyrights or other protections. At university management discretion, files, data or communications may be reviewed as necessary; therefore, individuals are not entitled to any expectation of privacy with regard to their files, data or communication.

III. Never share your university messaging credentials with others

A. Working with Mobile Devices

A variety of cell phones, personal digital assistants (PDAs) and other mobile devices may be used to access university messaging resources. However, special care must be taken in selecting external providers and configuring mobile devices for accessing your university email. Keep the following rules in mind:

1. Your JMU email account may not be redirected (mass forwarded) to an external cell/service provider for ease of access.
2. Providers/devices that use Microsoft ActiveSync (WindowsMobile, iPhone/iPod Touch, and some Palm Mobile Devices) to access your JMU account are preferred. These services generally let you access your email directly using your existing JMU credentials. Employees should not sync/access JMU messaging services using providers that require you to store your JMU account password/credentials with them.
3. Depending on the particular service and its configuration, messages and message-related content such as contacts, calendar and task items, and attachments may be synchronized as well and often present a security concern. Encryption and device passwords should be used as safeguards.
4. Detail about the university's mobile device support and configuration requirements is available at:
<http://www.jmu.edu/computing/helpdesk/selfhelp/exchange/exchangefaq.shtml#Mobile%20Devices/>

Last Updated: 6/1/10