Electronic Messaging Standard

November 2023

Purpose:

The purpose of this standard is to outline the principles and expectations that govern individual and common use of JMU's electronic messaging systems. In accordance with University Policy 1209 – Electronic Messaging, this standard applies to all individuals and/or technical mechanisms that use the University's information technology resources for electronic messaging functions.

Standard:

Shared Resource

Messaging systems use many networks and computing resources that are shared by the campus community as well as services shared by the world. Electronic messaging services should address a particular need and 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 - Appropriate Use of Information Technology Resources). Electronic messaging services available to JMU faculty, staff, students, and affiliates and their intended purpose include the following:

- E-mail and instant messaging: person-to-person
- E-mail list: small group discussions
- SMS: person-to-person, person-to-large groups, information distribution
- List, forum, chat services: large group discussions
- Website: public information distribution

University messaging credentials should never be shared with others.

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.

Privacy

Email: While privacy cannot be ensured on all systems in a particular message route, Information Technology (IT) will work to ensure 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 ensured. 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.

SMS: JMU does not sell personal information. The University may send JMU-related direct marketing communications as permitted by law including information about JMU, announcements, updates, alerts, support, and administrative messages, and may share personal information with third-party companies and individuals that are authorized by JMU to provide messaging services on behalf of the University.

Additional information on JMU's Commitment to Privacy can be seen at https://www.jmu.edu/policies/web-privacy-statement.shtml.

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 (See Guidelines for Data Storage and Collaboration).

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.

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.

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 an 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 used 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 recipient. Individuals who use resources such as forums/newsgroups, email lists, chat services, etc. must 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 the discretion of university management, files, data, or communications may be reviewed as necessary; therefore, individuals are not entitled to any expectation of privacy regarding their files, data, or communication.

Mobile Devices

A variety of cell phones 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 university email. The following rules apply:

- JMU email accounts may not be redirected (mass forwarded) to an external cell/service provider for ease of access.
- Providers/devices that use Microsoft ActiveSync (iPhone/iPad/Android) to access JMU accounts are preferred. These services generally provide access to email directly using existing JMU credentials. Employees should not sync/access JMU messaging services using providers that require the storing of JMU account passwords/credentials with them.
- Depending on the particular service and its configuration, messages and message-related content such as contacts, calendar, tasks, and attachments may be synchronized as well and often present a security concern. Encryption and device passwords should be used as safeguards.
- SMS messages from personal devices are prohibited for university business.