STATUS: (X) FINAL ( ) DRAFT
EFFECTIVE DATE: 10/11/99
REVISED: 11/10/2020

BULLETIN NO.: 2.100
PAGE: 1 OF 6

SUBJECT: Electronic Mail

SECTION: Information Management

I. PRACTICE

A. Statement of Policy and Purpose

The Department of Military Affairs (DMA) has a computer information system which supports electronic mail (email) that is provided to assist staff in their daily work routine. Staff who use electronic mail services are expected to do so responsibly, to comply with state and federal laws, with this and other departmental policies, and with normal standards of professional and personal courtesy and conduct.

The DMA respects the privacy of email users and does not routinely inspect, monitor, or disclose electronic mail without the user's consent. Nonetheless, the department may deny access to electronic mail services and may inspect, monitor, or disclose electronic mail when consistent with law, when there is reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs.

Email messages are used like paper memos, letters, and reports to conduct agency business but may also be casual communications, like telephone conversations. Such transitory messages have only momentary communicative value and lose their administrative value as soon as read. Email often provides for quick and easy distribution of important business-related materials that improve input into decision-making and greater distribution of information and decisions.

Some email messages are public records under Wisconsin Statutes. Others are not. Email messages that are public records should be retained in accordance with state statutes and approved records disposition authorizations (RDAs) for the appropriate record series. Email messages that are of only momentary communicative value need not be saved. Contents and business use are the keys to making such decisions.

End users are responsible for managing the email messages they receive and for properly identifying, classifying, retaining, and disposing of messages, in accordance with statewide and agency policies.

Conscientious use of our email system will avoid overburdening communications systems and avoid making it necessary to use scarce resources to eliminate service disruptions and system degradation that could easily be avoided.

B. Email Records

Public records: Email messages are public records like any other record – that is, they are public records if they are made or received by any state agency worker in connection with the transaction of public business.

Open records: Email messages that are public records are subject to the open records law and need to be filed and stored in such a way that they can be located, accessed, and provided to requesters for inspection and/or copying, as specified in law. Email is *not* confidential, unless access to a record is limited under law.

Records retention and disposition: Email records should be retained for the period appropriate to their content. Email messages should be disposed of in accordance with the approved record disposition authorizations (RDAs) for records of like content in other media. Email messages of limited communicative value can be deleted once they are no longer needed.

Duplicates: Email as a medium promotes communication to multiple users with great ease. Consequently, email systems frequently contain duplicates of a record. In general, if a user takes official action related to a message and the message is needed for documentation, it should be retained as a record. Otherwise, a duplicate is a nonrecord that can be deleted.

C. Ownership and Use

Ownership: The email system is government property. Email messages are the property of the government, not its employees, vendors, or customers. End users are obliged to follow agency work rules with respect to use of the email system.

Abuse: No one may use another employee's email ID to send messages without that person's express permission. Any other use of an ID is misrepresentation.

II. PROCEDURE

A. Appropriate Use of Email

Work rules covering such areas as recordkeeping, use of state property, and communications with others also apply to email. Failure to adhere to such general work rules when using email can be grounds for disciplinary action. Employees must use email resources responsibly and abide by normal standards of professional and personal courtesy and conduct. Email, or other telecommunications systems, will not be used in a way that would interfere with official duties, reflect adversely upon the organization (such as uses involving pornography, chain letters, unofficial advertising, soliciting, or selling via email, and other uses that are incompatible with public service), or further any unlawful activity or personal commercial purpose.

Email will not be used in a manner that overburdens telecommunications systems. Users should not send email that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing or telecommunication facilities, or unwarranted or unsolicited interference with others' use of email or email systems. Such interfering uses include, but are not limited to, the use of email services to:

1. Send email chain letters.

2. "Spam." That is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited email.

3. Broadcast unnecessary advertisements of services.

4. "Letter bomb." That is, to send the same email repeatedly to one or more recipients to interfere with the recipients use of email.

5. Broadcast email messages of daily quotations, jokes, or other similar transmissions.

6. Broadcast unsubstantiated virus warnings from sources other than authorized system administrators.

7. Direct messages to large audiences and send repeats of the same messages as reminders.

8. Send animation, sound, or other image files as attachments that have no official purpose.

Email is provided at department expense to serve the business needs of the agency. Employees may use email for occasional and incidental personal communications provided that such use does not directly or indirectly interfere with the department's operation of the computing facility or electronic mail messaging service; burden the department with additional incremental costs; interfere with the email user's employment or other obligations to the department; or cause unwarranted interference with the use of email or the email system by others. Incidental purposes may include announcing work-related social events, extending a luncheon invitation, or contacting family or others about work-related transportation, work hours, or family emergencies, and so on. Employees should delete any message that is not a state business record, immediately after reading the message.

No employee may misrepresent someone else by using that person's email ID to send messages without that person's express consent and permission. Generally, an employee may not access and read another employee's email messages without express consent.

Employees should take steps to assure that department documents are available to others as needed. The department will not monitor electronic mail messages as a routine matter but will respond to legal process and fulfill its obligations to third parties. The department will inspect the contents of electronic mail messages in the course of an investigation triggered by indications of impropriety or as necessary to locate substantive information that is not more readily available by some other less intrusive means. The department reserves the right to access and disclose the contents of employee electronic mail messages but will do so only when there is a legitimate business or legal need.

B. Email Records

All email messages, including personal communications, could be subject to investigatory review or discovery proceedings in legal actions. Some courts have set legal precedents for making use of email communications as evidence. Haphazard filing procedures, incomplete recordkeeping, and the use of informal language in email messages may misrepresent the department in legal proceedings. As with other records, no email record may be destroyed after someone requests it until the request is granted, 50 days have elapsed following denial of the request, and litigation on the record's availability is complete and any court order has been complied with.

Email records also fall within the definition of "record" under the Wisconsin Public Records Law (s. 19.32(2), Wis. Stats.). Electronic mail records are subject to the presumption of complete public access. Written open records requests for employee email for a particular day or week will be honored.

C. Archiving and Retention

The DMA does not maintain central or distributed electronic mail archives of electronic mail sent or received. Electronic mail is normally backed up to ensure system integrity and reliability, not for the sole purpose of future retrieval, although backups may at times serve the latter purpose incidentally. The IT staff is not required by this policy to retrieve email from such backup systems upon the originator's request.

Attachments (files created in other applications software) are an integral part of email. For email documentation to be adequate, complete, and reliable, the email message, any attachments, and the transmission history (routing, date and time) may be needed. The use of different applications software among users and senders can lead to unopenable or garbled files for the receiver. The growing use of standard software in state agencies is assisting to solve this problem.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms, such as embracing compound documents, usage of digital technology, voice recognition, audio and video media, and imaging in addition to text. Furthermore, in the absence of the use of authentication systems, it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email records that have administrative, legal, fiscal, historical, or audit significance should be saved beyond the designated system retention to either a desktop folder or a shared file in a manner that facilitates access. Staff should, on a regular basis, review email and delete items that do not need to be retained. Such maintenance can reduce the burden on servers and improve the overall performance of the system, yet ensure that the requirements of records management are observed. The state IT staff is available for assistance or technical advice on how to assure that needed email records are preserved.

To retain records and keep them accessible, it's a good idea to create a set of email folders that mirrors your paper filing system. Today, records can come in on a variety of media, and it is not always easy to keep together all materials related to a subject or case. Staff can adopt procedures for addressing this issue, such as printing out email messages and filing them with related paper documents. Once an email message, including its routing information, has been saved in another system, it may be deleted from the email system.

D. Disclosure and Restricted Access Without Consent

The electronic mail system is provided at department expense to conduct state business. Incidental and occasional personal use is permitted within the department, but such messages will be treated no differently from other messages.

The department has authority to obtain access to the contents of any employee's email files without the permission of the employee. Such circumstances include unavailability of the employee, a potential disciplinary issue, or preservation of email from possible destruction.

The department will permit the inspection, monitoring, or disclosure of electronic mail without the consent of the user of such email when required by and consistent with law, if there is reason to believe violations of law or department policy have taken place, when performing periodic checks for excessive personal use of email, and for meeting time-dependent, critical operational needs.

Attachment:

See P&P No. 2.110 for Receipt Certification