



270 FW 9

Email Use and Management

Supersedes Director's Order 103, 09/14/98
Date: July 23, 2008
Series: Information Resources Management
Part 270: IT Program Management
Originating Office: Division of Information
Resources and Technology Management

[PDF Version](#)

9.1 What is the purpose of this chapter? This chapter establishes the policy for using the Service's electronic mail (email) system and preserving email records.

9.2 What is the policy? All Service employees using the Service email system must:

- A. Follow the requirements in this chapter,
- B. Preserve email records that document our organization, functions, policies, decisions, procedures, and essential transactions, and
- C. Ensure that contractors using the Service email system meet the requirements in this chapter.

9.3 What is the scope of this chapter? This chapter applies to all users of the Service email system, regardless of the device used to access the system (i.e., PC, laptop, or Personal Digital Assistant (PDA)).

9.4 What are the authorities for this chapter?

- A. Federal Records Act ([44 U.S.C. 3301](#)).
- B. [385 DM 7](#), Electronic Mail Systems.
- C. [Department of the Interior Internet Acceptable Use Policy](#), 05/23/97.
- D. [384 DM 1](#), Records Disposition.

9.5 Who is responsible for email use and management?

A. The Assistant Director – Information Resources and Technology Management (IRTM):

- (1) Certifies that the Service uses an accredited email system, and
- (2) Ensures there are policies and resources in place to manage the email system.

B. The Chief, Division of IRTM:

- (1) Is the email system owner, overseeing daily operations and delegating authority for daily operations at the Regional level to Regional Chief Technology Officers, and
- (2) Issues policies for the email system, including email etiquette, appropriate use, and security warnings related to email.

C. Regional and Program Chief Technology Officers ensure that the employees in their respective Regions/programs follow this policy.

D. The Service Records Officer:

- (1) Prepares policies and procedures about email records;
- (2) Provides advice, training, and guidance on retaining email records Servicewide; and
- (3) Serves as the liaison with the Regions and the National Archives and Records Administration (NARA) for retaining and disposing of email records.

E. Managers and supervisors:

- (1) Ensure their employees follow the requirements in this chapter.
- (2) Deal directly with situations involving misuse or abuse of email.
- (3) Ensure that all employees are aware that their email messages are not private and the public may perceive them as official expressions of the Service.
- (4) Ensure that messages from their office to non-Service addresses, especially listservers and newsgroups accessible on the Internet, adhere to regulations.
- (5) Require that all of their employees and contractors who use the email system:
 - (a) Complete [FWS Form 3-2212](#), Automated Information System Statement of Responsibility (SOR).
 - (i) Employees and contractors must complete the SOR form before they can have access to any Service IT system.
 - (ii) Managers/supervisors should retain a copy of the signed form and give one copy to the user's Regional IT Security Manager (RITSM) and the original copy to the employee.
 - (b) Take annual Security Awareness Training; and
 - (c) Complete [FWS Form 3-2211](#), Password Control Document (also see 270 FW 7).
- (6) Notify system administrators immediately when an employee leaves the Service.

F. All employees must:

- (1) Read and adhere to our [Acceptable Use Security Standard \(Rules of Behavior\)](#) and [270 FW 7, Automated Information System Security](#);
- (2) Complete and sign [FWS Form 3-2211](#), Password Control Document to be eligible for an email and network account;
- (3) Take Security Awareness training before accessing any Service IT system and give the course certificate to their supervisor. Employees must take this training annually.
- (4) Complete and sign [FWS Form 3-2212](#), Automated Information System Statement of Responsibility (SOR).
- (5) Learn records management principles so they can distinguish between records and nonrecords (see [section 9.12](#) for more information). Take Privacy Act and Records Management training annually.
- (6) Follow the requirements in this policy. Employees who misuse email are subject to disciplinary action.

(7) Report misuse of email to the appropriate manager.

9.6 What are the required practices and prohibitions for email?

A. Required Practices. You must:

(1) Limit the number of large files you attach to email messages and choose “Reply without Attachments(s)” whenever possible. Do not email attachments over 25 MB; our email system will reject the message and notify you it was not sent. We transmit messages over 5 MB after 6:00 p.m.

(2) Use good judgment to limit “Reply to All” email responses by replying to only those people who need to know.

(3) For emails with attachments, reply to them without the attachments and forward them without attachments whenever possible.

(4) Maintain your email database size so that it does not get too large by regularly deleting messages and archiving messages you need to keep (see [section 9.11](#) for more information). The majority of users should maintain a database that is no bigger than 125 MB or at the limit set by your Region.

(5) Use the “Out-of-Office” agent when you plan to be out for a day or longer.

(6) Review email messages as frequently as your supervisor requires and act on them promptly.

B. Prohibitions. You must not:

(1) Send “All Employee Messages” unless you are authorized to do so (see [section 9.7](#) for more information).

(2) Use unnecessary or animated graphics in your email messages.

(3) Use profanity, racial or ethnic slurs, sexually harassing language, or slander.

(4) Use the Service email system for:

(a) Transmitting sensitive information; material of a personal, private nature; or information that is part of a Privacy Act system unless the information is encrypted (see [section 9.9](#) for more information).

(b) Any form of partisan politics.

(c) Personal commercial activities, any venture related to private gain or profit, and personal fundraising activities. This includes offering services or merchandise for sale, ordering non-work related services or merchandise from online vendors for a commercial purpose, and solicitations for event sponsorship and sales of merchandise.

(d) Religious activities, including newsletters, fundraising, proselytizing, prayer exchange, or activities related to the management of a religious institution.

(e) Any illegal activity and any activity prohibited by other Federal or Service policy or that could bring discredit to the Service.

(f) Accessing, retrieving, or printing text or graphics that exceed the bounds of generally accepted standards of good taste and ethics. Employees should avoid offensive language, sexual content, or any kind of content that would cause embarrassment if it were public knowledge.

(g) Any activity that may compromise the security of any Government information system or the information contained in that system.

9.7 What are the procedures for sending “All Employee” messages?

A. Only staff in the Director’s, Deputy Director’s, Assistant Directors’, and National Conservation Training Center Director’s offices may send “All Employee” messages.

(1) If an employee in a division or branch office wants to send an “All Employee” message, the employee first gets the necessary approvals in his/her division/branch. The employee then sends the draft message to their Assistant Director’s office for approval. Staff in the Assistant Director’s office send the email to all employees.

(2) If an employee wants the message to come from the Director’s or Deputy Director’s office, the employee first obtains the necessary approvals in his/her division. The employee then sends the draft message to their Assistant Director’s (AD) office for approval. The AD’s office sends it to the Director’s or Deputy Director’s office for approval and distribution.

B. Only use “All Employee” messages for:

(1) Official announcements,

(2) Policy decisions, and

(3) Items directly affecting employees.

C. Do **not** use “All Employee” messages for:

(1) Vacancy announcements, and

(2) Announcements about celebrations.

D. Regions may allow distribution of Regionwide messages.

9.8 What are the requirements for corresponding with the public using email?

A. Because the public may interpret email originating or forwarded from an “@fws.gov” address as an official agency position, employees must be careful to provide accurate and valid statements to the public using email. All email responses should reflect the Service’s commitment to provide excellent customer service.

B. All Headquarters divisions/offices and Regional offices must establish a general office email address for their Web sites using an “@fws.gov” address. More than one person should have access to the mailbox. Divisions/offices may link this mailbox to a database with an automated response agent that acknowledges receipt of the message and provides general information back to the originator.

C. Divisions/offices that publish documents in the Federal Register requesting public comments should offer the public a way to comment electronically. For documents published in the "Proposed Rules" or "Rules" sections of the Federal Register, you must solicit electronic comments through the [Regulations.gov](http://www.Regulations.gov) Web site. We only accept electronic comments

submitted via this Web site. For documents published in the "Notices" section of the Federal Register, you should include an e-mail address for submitting comments. You must always include a regular mail address for submitting comments.

D. To ensure a high level of customer service, employees should respond within 2-5 business days to email from the public or within whatever timeframes their supervisors determine are appropriate.

(1) If they cannot respond within the required timeframe, employees must at least acknowledge within that timeframe that they received the email.

(2) If the person who receives the email cannot address the topic or answer the question, he/she should:

(a) Acknowledge receipt of the email and copy the person who can provide the final response, or

(b) If unsure of where to refer inquiries or comments, send the email to the Office of External Affairs at contact2@fws.gov. This mailbox is primarily for public inquiries, not internal use.

(3) Employees should treat email the same as letters and faxes when determining whether or not we need a further detailed response (see [282 FW 1-4](#)).

E. Employees must file email exchanges with the public as records in an appropriate subject archive file (see [section 9.11](#) for more information about records).

9.9 What are the privacy considerations for using email?

A. All email transmitted using Service equipment and the Service email system is subject to monitoring. Such communications are not private. Your supervisor, email managers, or other support staff may review email messages, as necessary. Employees authorized to investigate Service personnel also may review email, as necessary.

B. Employees may not use the Service email system to transmit sensitive information; material of a personal, private nature; personally identifiable information; or information that is part of a Privacy Act system unless the information is encrypted. Encryption prevents people from intercepting and reading the information. For information about how to encrypt documents, ask your IT specialist or contact the Division of IRTM.

C. Employees should not enter their home telephone numbers, personal cell phone numbers, home addresses, or other personal information in the email system directory.

9.10 May Service employees use the Service email system for personal communications?

Employees may use the Service email system on non-duty time for limited personal communications if:

A. The cost to the Service is negligible.

B. The email(s) do not cause congestion, delay, or disruption of service to any Government system or equipment (e.g., by transmitting large attachments).

C. Employees do not represent themselves as acting in an official capacity in personal email messages.

D. Employees do not send large digital pictures, videos, and audio files (i.e., larger than 5 MB) in personal email messages.

E. They are careful when giving out their Government email address, particularly when registering or subscribing at Internet sites. Registering on Internet sites often results in automatic email traffic that may strain our network resources.

9.11 Do Service employees have to treat email messages the same as other Federal records?

A. Yes. Our email is subject to laws governing public access, including the Freedom of Information Act, the Privacy Act, the Paperwork Reduction Act, and the Federal Advisory Committee Act. A court may subpoena email if it is relevant to ongoing litigation, and its loss can be detrimental to our credibility in court.

B. All email messages that we use to conduct agency business are records of the Service (see [282 FW 4](#)). You should retain them according to our Records Disposition schedule (see [283 FW 2](#)). Do not delete electronic records unless you electronically archive them or print and file them.

C. Following are a few examples of the types of email that are records:

(1) A series of email messages that show the reasoning behind revisions to a position paper that two or more employees are developing.

(2) An email message from a Directorate member requesting a revision to a draft policy that a division sent out for Directorate review.

(3) A series of email messages between a private landowner and a Refuge manager about the Service acquiring land.

(4) An email message from a Department official requesting a cost-benefit analysis of a management decision.

D. Following are a few examples of the types of email that are not records and that employees may delete at their discretion:

(1) Information that is not business-related and is purely personal in nature (lunch meetings, personal appointments, and family-related email);

(2) Duplicate information already documented and retained in a record copy (e.g., copies of an all-employees memo);

(3) Copies of reference information that you did not create or use in a business context (e.g., a courtesy copy of a *Government Executive News* article, retirement newsletters, vendor product information). Reference material we use for decisionmaking and sent as an attachment is a record.

9.12 What are the procedures for preserving email records? Unless other procedures have been established to preserve email records (e.g., for litigation involving a specific case or special procedures field offices establish to accommodate their systems), employees should follow the following steps to preserve email records:

A. Establish an electronic archive file in the email system for every significant project, case, issue, or program on which you work.

B. When you receive an email record, print it and any attachments, and file the printout according to your program/office's filing system.

C. File the email record and any attachments in the appropriate archive file. Do not use your active email database to maintain and file records.

D. Promptly delete email messages (within 30 days) that are not records.

(1) Email administrators retain email backup tapes for at least 30 days.

(2) During that time, the deleted messages are temporary records that are subject to review and could be released under the Freedom of Information Act (FOIA).

(3) You must not delete any email message, including any message on a backup tape, that is a record or involved in an active FOIA request, appeal, or litigation.

9.13 Where can employees get more information about using the Service email system, preserving email, and Government records? Employees may visit the following Web sites for more information:

A. [Division of Information Resources Technology Management \(IRTM\).](#)

B. [Service Records Management.](#)

C. [Service Privacy Act Information.](#)

D. [Service FOIA Officers](#)

E. [Ethics Office](#)

For information on the content of this chapter, contact the Division of Information Resources and Technology Management. For information about this Web site, contact [Krista Holloway](#) in the Division of Policy and Directives Management.

[Directives Home](#)

PDM Web sites: [Centralized Library of Servicewide Policies](#) | [FWS Forms](#) | [PDM Services](#)

[Privacy, Disclaimer and Copyright Information](#) | [Information Quality Act](#)

[U.S. Fish and Wildlife Service Home Page](#) | [Department of the Interior](#) | [USA.gov](#) |
[About the U.S. Fish and Wildlife Service](#) | [Accessibility](#) | [Privacy](#) | [Notices](#) | [Disclaimer](#) | [FOIA](#)