

## **ADDITIONAL RECORDS-RELATED INFORMATION**

**AUTHORITIES** - This guide is based on the following Federal authorities:

- 36 CFR, Parts 1220, 1222, 1226, and 1234;
- 44 U.S.C. Chapters 21, 29, 31, and 33 (Federal Records Act (FRA));
- 18 U.S.C. Section 641 (Appropriate use of public money, property or records);
- 18 U.S.C. Chapter 101, Section 2071, (Penalties for misuse of records);
- 5 U.S.C. 552 (Freedom of Information Act);
- 5 U.S.C. 552a (Privacy Act); and
- Federal Information Resources Management Regulations, Section 201-21.601 (Use of Government Telephone Systems).

---

**Legal Penalties.** Federal employees who willfully and unlawfully conceal, remove, mutilate, obliterate, falsify, or destroy Federal records shall be fined not more than \$2000, and/or imprisoned not more than 3 years, and forfeit Federal office, and be disqualified from holding Federal office. (18 U.S.C. Chapter 101, section 2071.)

**Appropriate Use of E-Mail.** While electronic mail systems often replace telephones to relay information to individuals, the Network may not be used for unofficial personal matters except for those approved uses of Government telephone systems identified in [Appendix C](#) (e.g. messages concerning telephone calls from home or doctors). Private or other sensitive information should not be disclosed or transmitted via the Network unless authorized to do so.

Messages and loose language could be taken out of context and lead to inappropriate or potentially damaging conclusions. The use of profanity, racial or ethnic slurs, sexually harassing language, slander, and other such language is as inappropriate in E-Mail as in any other medium. Network storage requirements are also another issue related to the appropriate use of E-Mail. Users need to distinguish records from non-records on the network, properly preserve the records, and promptly dispose of non-records as soon as they have fulfilled their purpose.

**Use of E-Mail Backup Tapes:** Network backup tapes are for system recovery or for restoring information which has been deleted in error. Backup tapes do not have the features required for agencies to use as a record storage methodology to ensure retrievability and easy access to specified documents. However, E-Mail system backup tapes are routinely stored and can be used in court as evidence.

**Records Disposition Requirements.** Federal records are Federal property and are appraised by agencies for their administrative, fiscal, and legal value in conducting official business. Records are also appraised by NARA for potential enduring value beyond the needs of the agency. The appraised value determines when and how the records should be disposed. Generally records are either destroyed after a specific retention period or they are transferred to the custody of NARA for permanent retention.

**Records schedules** are legal documents governing the retention and disposition of records. Unscheduled records must not be disposed of until approved disposition authority has been obtained from the Archivist of the United States. Network users should become familiar with schedules governing records they create or maintain to ensure proper records disposition.

Contact the appropriate Records Management Officer ([see Attachment 2](#)) for copies of approved records schedules and for any additional needed records management assistance.

**Adequate Documentation.** Once Network users determine that a note, message, memorandum, or other electronic communication is a Federal record, that material **must** be saved in a way that includes **all** the pertinent information contained therein (e.g., date, time, and mailing lists). For example, if a confirmation to a message (record) is requested by the author, a copy of the confirmation should be generated and filed with the record.

See [Appendix B](#) for definitions of additional terms used in this guide.

---

**FREEDOM OF INFORMATION ACT REQUIREMENTS.** E-Mail files within the Network may contain information that must be disclosed to the public, upon request. The Freedom of Information Act (FOIA) grants to any individual the right to access Federal agency records. The FOIA permits an agency to withhold from the public only those records that fall within the scope of one of the nine exemptions listed on page 9. Under the Department's FOIA regulations (43 CFR Part 2) information falling within an exemption may be withheld only if (1) disclosure is prohibited by statute or Executive Order, or (2) disclosure would be harmful to an interest protected by the exemption, (i.e., an individual, a submitter of confidential commercial or financial information, or the Government). **Records that are the subject of active FOIA requests or appeals procedures may not be deleted or otherwise disposed of even if they are authorized for destruction by an approved record schedule.**

**FOIA Requests.** The Department must respond directly to requests for reasonably described records within 10 working days of receipt of a FOIA request. FOIA requests are received from private citizens, corporate bodies with commercial interests in Departmental decisions, public interest groups, and representatives of the news media. Network users may be asked to search their electronic files for records responsive to FOIA requests and to provide the requester with copies of all non-exempt records. Material deemed to be "non-record" under the FRA may be a record for the purposes of FOIA.

**FOIA Appeals.** Under the Department's regulations (43 CFR 2.18), requesters have the right to file an administrative appeal with the Department when:

- Records have been withheld either partially or entirely;
- a request has been denied for failure to describe requested records or for other procedural deficiency or because requested records cannot be located;
- a fee waiver request has been denied; or
- a response to a request has not been communicated to the requester within the prescribed time limits.

If the requester is not satisfied with the outcome of the Department's determination on the appeal, the requester may sue the Department. During the FOIA request, appeal, or litigation process the requested records must be maintained in their entirety, even if they are authorized for destruction by an approved record schedule. Following completion of proceedings, the documents will be retained in accordance with "FOIA retentions" per the General Records Schedule.

**FOIA Exemptions:** Under the FOIA there are nine exemptions which serve as a basis for withholding information from the public. The nine exemptions are listed below and are discussed in detail in the FOIA Handbook (383 DM 15). In case of doubt in response to a FOIA request, contact your bureau FOIA Officer.

Exemption 1 - Matters of National Defense or Foreign Policy

Exemption 2 - Internal Personnel Rules and Practices

Exemption 3 - Information Exempted by Other Statutes

Exemption 4 - Trade Secrets, Commercial or Financial Information

(Confidential Business Information)

Exemption 5 - Privileged Interagency or Intra-agency Memoranda or Letters

Exemption 6 - Personal Information Affecting an Individual's Privacy

Exemption 7 - Records Compiled for Law Enforcement Purposes

Exemption 8 - Records of Financial Institutions

Exemption 9 - Geological and Geophysical Information Concerning Wells

---

**PRIVACY ACT REQUIREMENTS.** The Privacy Act of 1974 grants access and amendment rights to individuals for records about themselves, within systems of records that are retrieved by name or personal identifier. The Act requires agencies to ensure records are accurate, relevant, timely, and complete, and it protects them from unauthorized disclosure.

**Records Retrieval.** Agencies maintaining systems of records retrieved by personal name or identifier are required by law to alert individuals on whom the records are maintained of the procedures for accessing and amending these records. This requirement is carried out through the Federal Register process. The Privacy Act also requires agencies to comply with a variety of recordkeeping requirements.

**Records Disclosure.** Records within systems protected by the Privacy Act must not be created, maintained, disclosed, or transmitted over the Network except as authorized by the Act.

**Non-record copies** of approved Privacy Act systems of records, if needed, may be stored on diskettes that are maintained in secure areas, or on a user's password protected local disk drive.

---

[Appendix B - Additional Definitions](#)

[Appendix C - Examples of Calls Necessary in the Interest of the Government](#)

[ATTACHMENT 2 - List of Departmental Records Managers](#)