



United States Department of the Interior

NATIONAL PARK SERVICE

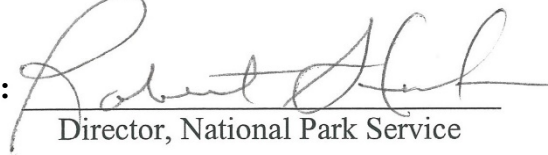
1849 C Street, N.W.

Washington, D.C. 20240

IN REPLY REFER TO:

DIRECTOR'S ORDER #5: PAPER AND ELECTRONIC COMMUNICATIONS

Approved:


Director, National Park Service

Effective Date:

July 10, 2000

Sunset Date:

JUL 10 2004

NPS-5, "Correspondence Guideline," and Special Directive 95-13, "Electronic Mail," are superseded and replaced by this Director's Order and the Washington Office Correspondence Manual.

Table of Contents

- | | |
|--|---|
| 1. Background and Purpose | 9. Relationship to Records and FOIA |
| 2. Authority and Related Guidance | 10. Relationship of Paper to Electronic Media |
| 3. Scope | 11. Congressional Communications |
| 4. Definitions | 12. Accuracy |
| 5. Responsibilities and Delegations | 13. Security |
| 6. Employee Access | 14. Personal Use |
| 7. Privacy Expectations | 15. Inappropriate Use |
| 8. Emergency Communications and Mission Critical Designation | |

1. Background and Purpose

The National Park Service is highly dependent on a wide variety of communications media in the performance of its mission. Paper correspondence, electronic mail (e-mail), Internet mail, and facsimile transmissions are used to communicate both internally, and with organizations outside the National Park Service. The Service also uses Intranet for important internal communications. In both routine and emergency situations, e-mail is now considered essential, and the Service is coming to rely increasingly on the information at Intranet and Internet sites.

This Director's Order describes the responsibilities and requirements for written communication in all media, both electronic and in paper, and both within and outside the National Park Service. It particularly addresses the new world of issues related to written communications in electronic form on e-mail, Internet, and Intranet, including personal

use of these government facilities, appropriate and inappropriate behavior, the relationship between paper media and these electronic media, and privacy considerations. Electronic publishing of information by posting it on the World Wide Web or other Internet or Intranet locations is addressed in Director's Order #70: Internet and Intranet Publications, and its associated handbook.

2. Authority and Related Guidance

2.1 General authority to issue this Director's Order is contained in 16 USC 1 through 4 (the National Park Service Organic Act), and the delegation of authority contained in Part 245 of the Department of the Interior (DOI) Manual (DM).

2.2 The following laws and guidance direct the National Park Service in its use of electronic communications:

- DOI IRM Bulletin 1996-006 (July 25, 1996): "Policy and Guidance for Managing the Creation, Retention, and Disposition of Electronic Mail Documents," except where this bulletin has been superseded by guidance from the National Archives and Records Administration.
- DOI IRM Bulletin 1997-002 (May 12, 1997): "Department-wide Standards for the Retention of Electronic Mail (E-mail) System Messages and E-mail System Backup Tapes."
- DOI Policy on Limited Personal Use of Government Office Equipment (June 14, 2000).
- The Freedom of Information Act (5 USC 552; PL 89-554, 90-23).
- The Privacy Act of 1974 (5 USC 552; PL 93-502).
- 5 USC 7321-7326 (the Hatch Act), which, among other things, prohibits Federal employees from using appropriated funds to lobby Congress or to encourage others to do so.
- The Federal Records Act (including amendments and additions) is the basic law regarding Federal government recordkeeping responsibilities and activities. (Chapters 29, 31, 33 of Title 44, US Code.) Basic regulations that govern agency recordkeeping activities (including National Park Service recordkeeping), are contained in 36 CFR Parts 1220-1238.
- The Chief Information Officers' Council's recommended Executive branch model policy/guidance, "Limited Personal Use of Government Office Equipment Including Information Technology," approved by the General Services Administration (GSA) May 19, 1999. See also, 410 DM.

2.3 The following National Park Service guidance addresses related activities and material:

- Director's Order #19: Records Management, and its accompanying materials are the primary guidance within the NPS for the management of records, including electronic records.
- Director's Order #70: Internet and Intranet Publishing, and its accompanying handbook, are the primary guidance for publishing information on the Internet and Intranet (through ParkNet and the World Wide Web).
- The Washington Office Correspondence Manual describes correspondence style for certain types of correspondence, including Congressional correspondence and correspondence for the Director or Deputy Director's signature, and the controlled correspondence process.

3. Scope

This Director's Order applies to all National Park Service employees, and to all non-employees who may regularly or occasionally use the National Park Service's information technology equipment, networks, and/or systems. This includes (but is not limited to) other Federal, or State, employees, volunteers, cooperating associations, friends groups, concessioners, and contractors. This Director's Order also applies to both professional and personal use of NPS information technology equipment, networks and systems.

4. Definitions

4.1 "Correspondence" is defined as all written communication received from, or going to, the National Park Service. This includes letters received by any means of transmission, including standard mail, e-mail, or facsimile. "Controlled correspondence" is correspondence that has been designated by the Secretary or the Director as of such importance as to warrant tracking through a central headquarters office.

4.2 "Intranet" is defined as the closed use of Internet technologies for communication of information within the National Park Service.

4.3 "Mission critical system" is defined as: "those systems that, when their capabilities are degraded, the organization realizes a resulting loss of a core capability, or life or property are threatened." (This is the definition used by DOI.)

4.4 "Minimal additional expense" means situations where the NPS is already providing equipment or services, and the employee's use of them will not result in any additional

expense to the government, or will result in only normal wear and tear, or will use small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include: using a computer printer to print a few pages of material; infrequently sending personal e-mail messages; or limited use of the Internet for personal reasons.

4.5 “Information technology equipment” means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.

4.6 “Employee non-duty time” means time when the employee is not expected to be addressing official business. This includes: their own off-duty hours, such as before or after a workday (subject to local office hours); lunch periods; authorized breaks; or weekends or holidays (if their duty station is normally available at such times).

5. Responsibilities and Delegations

5.1 Directorate

The Director, Deputy Directors, Regional Directors, Associate Directors, and heads of offices reporting to the Director/Deputy Directors are responsible for ensuring that all correspondence, regardless of medium, is responded to accurately, efficiently, professionally, and within acceptable and established timeframes.

5.2 Director

The Director sets the style for all written and electronic correspondence, both with external persons and organizations and internally within the National Park Service, that is signed by the Director and Deputy Directors. Particulars of this style are described in the Washington Office Correspondence Manual.

5.3 Associate Director for Administration

The Associate Director for Administration maintains this Director’s Order and the Washington Office Correspondence Manual, manages the controlled correspondence process, and consults with the Chief of the Office of Legislative and Congressional Affairs on determining procedures for Congressional communications.

5.4 Associate Director for Professional Services

The Associate Director for Professional Services is responsible for the data communications infrastructure that supports NPS e-mail, and Intranet and Internet applications (see Director’s Order #70).

5.5 Regional and Associate Directors

Regional and Associate Directors are delegated authority to determine the style for all written and electronic correspondence in their jurisdictions.

5.6 Supervisors

Supervisors are responsible for ensuring that designated employees have access to e-mail (including bulletin boards), Internet and Intranet (see section 6), and for ensuring distribution of information to employees without such access. Supervisors are responsible for ensuring local security of computer access by both employees and non-employees. Supervisors retain the right to restrict the use of e-mail and Internet/Intranet in circumstances deemed inappropriate, in cases of chronic misuse, or in cases that adversely affect other users or the larger communications infrastructure (see section 14.3).

5.7 Employees

Employees are responsible for (1) using correspondence, e-mail, Internet and Intranet legally, professionally, and considerately, and (2) abiding by all use restrictions within this Director's Order. Employees are responsible for being aware that communications in all media constitute government records, and for following all applicable records management procedures. Employees are responsible for security of access to their electronic identity as an NPS employee through their computer.

6. Employee Access

The mission of the NPS is served by having employees take full advantage of the business efficiencies made possible by e-mail, Internet, and Intranet.

6.1 An employee is considered to have full access to e-mail when he or she has a personal mailbox with the ability to receive and originate messages under his or her own name. Distribution of printed copies of e-mail messages does not fulfill the requirement of access to e-mail. An employee is considered to have full access to Internet/Intranet when they have a computer available to use for Internet access as part of their normal work environment, although not necessarily at their workstation.

6.2 Every effort should be made to give ALL employees, regardless of status, full, personal access to e-mail, Internet and Intranet. For individuals for whom full personal access is not practical or possible, generic or shared mailboxes and equipment may be provided.

7. Privacy Expectations

This section addresses the personal privacy of employees. Information that is normally considered confidential in the course of business remains confidential, whether on paper or on electronic systems, and is not changed by this section. Nothing in this section should be construed to give supervisors or any other employee rights to see information in electronic format that they would not be allowed to see in paper format (see section 10.6).

7.1 Employees utilizing NPS e-mail and Internet/Intranet systems do not have a right, nor should they have the expectation, of privacy. Use of NPS information technology equipment implies the consent of employees to disclosing the contents of any files maintained or passed through that equipment. To the extent that employees wish that their private activities remain private, they should avoid using NPS information technology equipment. Any use of NPS communications systems is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

7.2 By using NPS information technology equipment, employee consent to monitoring and recording is implied, with or without cause, including (but not limited to) use of Internet and e-mail. System managers do employ monitoring tools to detect improper use. Electronic communications may be disclosed within the NPS to employees who have a need to know in the performance of their duties. NPS officials, such as system managers and supervisors, may access any electronic communications.

8. Emergency Communications and Mission Critical Designation

The NPS e-mail, Intranet, and Internet systems, and the underlying information technology equipment that supports them, are all considered mission critical systems, and may be considered essential during emergency situations. The Intranet in particular is useful in meeting the continuity of operations requirement to have off-site reference information available in emergency situations. Managers should designate locations for the posting of official NPS information on an e-mail bulletin board and/or Intranet site (for internal communications), and/or Internet site (for external communications) for emergency situations as part of their emergency, incident, and continuity-of-operations planning, as appropriate.

9. Relationship to Records and FOIA

9.1 Paper correspondence, facsimiles, e-mail (in both printed and electronic form), Intranet, Internet, and system backups of all electronic media are all subject to the Federal Records Act and may qualify as official government records according to legal definitions. All are subject to the Freedom of Information Act (FOIA).

9.2 Since all e-mail and electronic documents (files or scanned) are subject to Federal records laws and regulations, any locations that are considering conversion to a “paperless office” system, or any internal system where the primary storage of records is electronic and not in paper form, must develop a records management plan for those electronic records as part of the system functional requirements, and implement it in conjunction with the primary system.

10. Relationship of Paper to Electronic Media

10.1 Incoming correspondence that is received via e-mail may be responded to using e-mail. E-mail should not be used for replies to correspondence that was received via other media (paper or fax), unless the author of the original correspondence permits its use.

10.2 Official internal communication within the National Park Service may be in any medium, including paper memoranda, Intranet posting, or e-mail. The sender must select the medium of communication they deem appropriate for the addressee.

10.3 E-mail must not be used to circumvent or avoid any standard routing procedures, approvals, or signature protocols already in place that apply to paper media.

10.4 Communication from any NPS manager, including the Director, to any NPS office or employee, carries the same weight in electronic form as in paper, and both are considered “official.” In some circumstances, paper media with an actual signature may be legally or ceremonially required. In these cases, while the original signed paper copy should be retained as the official record, paper copies are not required for addressees.

10.5 Each park or program office that hosts a web site on ParkNet must provide an e-mail address to which public inquiries may be directed. All inquiries must receive a timely and appropriate response, equivalent to that accorded paper correspondence.

10.6 Information that is considered confidential in paper form retains that confidentiality in electronic form and should be given the same measure of protection and security. This includes (but is not limited to) information normally kept confidential in the areas of personnel, equal opportunity, law enforcement, labor unions, protected under the Privacy Act (and 16 USC 5937), etc.

11. Congressional Communications

11.1 The Washington Office of Legislative and Congressional Affairs must review, prior to sending, any outgoing correspondence with members of Congress that is to be signed by the Director, and should be copied on any Congressional correspondence that involves substantive policy or controversial issues.

11.2 Under provisions of the Hatch Act (5 USC 7321-7326), Federal employees are expressly forbidden from using appropriated funds to lobby Congress or to encourage others to do so. Use of NPS e-mail, Intranet or Internet systems are all considered use of appropriated funds under this law. Lobbying activities include direct communications with Congress on an issue, as well as any encouragement of fellow employees to support or oppose any particular law or proposed legislative action, including electronic petitions and chain mail letters. Employees should consult with their ethics counselor for more information.

11.3 E-mail may be used to communicate with Congress only under those circumstances defined by Departmental policy governing corresponding with Congress in the conduct of official business, or when requested by the Congressional member.

12. Accuracy

The accuracy of all paper and electronic correspondence is the responsibility of the signatory. The accuracy of all Intranet and Internet information is the responsibility of the office that posts the information.

13. Security

Security concerns are of two basic types. First, NPS computers, information systems, and the data that they contain must be protected from hackers, misuse or corruption of data, unauthorized persons wanting to gain access to confidential information, etc. The second concern is the security of the National Park Service's image and reputation. Whenever someone sends a message or posts something to a website using an NPS computer, that information is "tagged" as coming from the National Park Service, and potentially may be interpreted as representing the National Park Service. The guidance in this section addresses both types of concerns.

13.1 Any person using a computer that has been assigned an Internet address within the NPS domain (an address ending in "nps.gov"), or who uses an NPS e-mail address, has an electronic "identity" as a National Park Service employee. The misuse of an NPS employee's electronic identity by a non-employee, or the inappropriate use by an employee, could compromise the security and reputation of the NPS. Each individual is responsible for understanding this and acting appropriately.

13.2 Each employee is responsible for the security of the personal e-mail and computer passwords assigned to him or her. Passwords should never be posted where they are visible to passers-by. Employees should only give their passwords to individuals who have a business need to access their systems.

13.3 Supervisors and managers are responsible for computer system and data security when non-NPS employees (such as contractors and volunteers) work in NPS locations, or use NPS equipment or systems.

14. Personal Use

14.1 Employees are permitted limited use of NPS information technology equipment, including e-mail and Internet, for personal needs, if the use does not interfere with official business, and involves minimal additional expense to the government. This limited personal use of government office equipment should take place during the

employee's non-duty time. [Note: Applying for jobs using Internet or e-mail is considered a personal use no different than any other, and is therefore permitted. However, the prohibition against using government stationery, envelopes and postage, for job applications or other personal use, is still in effect.]

14.2 It is the responsibility of employees to ensure that they do not give the false impression they are acting in an official capacity when using government office equipment for non-government purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used.

14.3 Employees have no inherent right to use NPS equipment for personal use. Personal use is considered a privilege, and may be specified, limited, or revoked at any time by appropriate NPS officials in order to meet management needs and mission objectives.

15. Inappropriate Use

The following are considered inappropriate uses of e-mail, Internet, Intranet, and other information technology equipment in the NPS, either for personal or professional use, and may result in limitation or loss of use of equipment, disciplinary or adverse personnel action, criminal penalties, and/or the employee being held financially liable for the cost of the improper use. Law enforcement personnel may access sites otherwise restricted by this section, if necessary, during the course of official investigations or intelligence-gathering activities. Technologies and software not specifically addressed here should be evaluated by managers against these use guidelines, and local conditions and resources (such as available bandwidth), to determine their appropriateness.

15.1 Any use that could cause congestion, delay, or disruption of service to any government system or equipment. With respect to e-mail, this may include large files, such as graphics, video, sound or other large file attachments; with respect to Internet, this may include "push" technology, "streaming," and other continuous data streams that can degrade the performance of the entire network. What is inappropriate will vary from location to location, depending on the amount of available bandwidth in that location.

15.2 Using NPS information technology systems as a staging ground or platform to gain unauthorized access to other systems ("hacking").

15.3 The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter.

15.4 Using NPS equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

15.5 The creation, downloading, intentional viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

15.6 The creation, downloading, intentional viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

15.7 Use for personal commercial gain, or in support of for-profit activities, or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services, day trading). Employees are specifically prohibited from using NPS equipment to support a personal private business; or to assist relatives, friends, or other persons in such activities.

15.8 The installation of personally owned software, e.g., tax preparation programs, computer games, etc.

15.9 Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

15.10 Posting NPS information to external newsgroups, external bulletin boards, or other public forums without authority. This includes any uses at odds with the NPS mission or positions, or that could create the perception that the communication was made in one's official capacity as an NPS employee, unless appropriate approval has been obtained.

15.11 The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked, or other material with intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

15.12 Any personal use that could generate more than minimal additional expense to the government (see section 4.4).

---- End of Director's Order ----