5.14 Use of Internet and Electronic Mail

A. Purpose

Email is a mechanism for official communication within Northwest Fire District. The District has the right to expect that such communications will be received and read in a timely fashion. Official email communications are intended only to meet administrative needs of the Northwest Fire District community.

The purpose of this policy is to promote professional, ethical and lawful use of Northwest Fire District's computer and network resources and to assure that:

1. Email will be used by the District in an ethical and considerate manner in compliance with applicable law and policies, including policies established by the District and with respect for the public trust through which these facilities have been provided.

2. Email users are informed about how concepts of privacy and security apply to email, as well as the applicability of relevant policy and law.

3. Disruptions to email and other services and activities are minimized.

B. Scope

1. This policy applies to:

a. All users of Northwest Fire District's computer and network resources.

b. All email services provided, owned or funded wholly or in part by Northwest Fire District.

c. All users and holders of District email systems or accounts, regardless of intended use.

d. All District email Official Records and/or Public Records in the possession of or generated by District employees and other users of email services provided by the District, regardless of whether the records were generated on District or non-District computers.

2. This policy does not apply to printed copies of email, but other law and policy may apply to such documents. Under Arizona records law and other state laws, information appearing in this format may need to be retained as Official Records or treated as State Publications under A.R.S. § 35-103. If the user prints out email Official Records (including transmission and receipt data) and retains them in hard copy according to approved District records management policies and retention schedules, the electronic copy may be deleted immediately.

3. This policy applies equally to transmission and receipt data including email headers, summaries, and addresses associated with email records and attached files or text.

C. Policy

1. Northwest Fire District provides computing and networking resources to all authorized employees. Access to the resources owned by the District is a privilege, which requires users to comply with certain responsibilities and obligations. All users must adhere to these policies and guidelines governing their use, which have been set forth by the District as well as local, state and federal laws, and respect the rights of others using a shared resource. (The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.)

2. Official District email accounts are available for all employees of Northwest Fire District. The addresses are all in the form "name@northwestfire.org." These accounts must be activated before the District can correspond with its employees using the official email accounts. The District email account is the only email account to be used on District computers unless prior approval is granted by MIS.

3. This policy clarifies the applicability of law and of other Northwest Fire District policies to email and internet use.

4. Northwest Fire District recognizes that principles of freedom, freedom of speech, privacy and confidentiality hold important implications for email and email services. This policy addresses these principles within the context of, and subject to, the limitations imposed by the District's legal and policy obligations.

D. Guidelines

1. **Acceptable Computer Use Guidelines**

The following specific usage guidelines are not intended to be comprehensive, but are to establish and clarify the intent of this policy.

a. **Use security measures to protect the integrity of information, data and systems.** Individuals must protect their computer systems and accounts by using passwords and installing anti-virus software consistent with management directives. MIS will keep such software, and the operating system and application security patches up to date. Users are only allowed to use identification codes and passwords as authorized and are responsible for safeguarding them.

b. **Users are responsible for safeguarding their identification (ID) codes and passwords and for using them only as authorized.** Each user is responsible for all email transactions made under the authorization of his/her ID, and for all network email activity originating from his/her data jack.

c. **Expectations about employee use of email.** Employees are expected to check their email on a frequent and consistent basis in order to stay current with District related communications. Employees have the responsibility to recognize that certain communications may be time critical.

d. **Respect copyright and intellectual property rights.** All users must abide by the U.S. Copyright Act, and the terms and conditions of any and all software and database licensing agreements. Even though a copyright notice is not present, any form of original expression fixed in a tangible medium is subject to copyright. Before using a copyrighted work, the user must either obtain the copyright owner's permission or an applicable exemption under the Copyright Act must exist. Copyright infringement exposes the user, and possibly the District to fines and potential criminal liability. Therefore, the District may refuse, suspend, or terminate computer and network access to anyone who violates the copyright law.

e. **Make only appropriate use of data to which you have access.** Employees may have access to data beyond what is generally available. Access to data may only be used in a way consistent with applicable laws, Northwest Fire District policies, and accepted standards of professional conduct. Those who have access to databases that include personal information must respect individual privacy and confidentiality consistent with applicable laws and District policies regarding the collection, use and disclosure of personal information.

f. **Respect and adhere to other departmental / Internet Service Provider's acceptable use policies.** Employees must adhere to the prevailing policies that govern a system or network when using a District computer to connect to that specific non-District system or network. This does not in any way release an employee's obligation to abide by established policies governing the use of Northwest Fire District computer systems and networks.

g. **Use computer and network resources efficiently.** Authorized employees may use Northwest Fire District's computer and network resources for individual personal purposes, given that such use does not:

   I. Interfere with the user's employment obligations.

   II. Unjustly hinder other employees' use or interfere with the District's operation of computing or network resources.

   III. Violate the law or other District policies.

h. **Northwest Fire District retains the right to set priorities on the use of the system.**

2. Violations of Acceptable User Guidelines:

a. Using a computer account and/or obtaining a password that the employee is not authorized to use.

b. Using the District network to gain unauthorized access to any computer system.

c. Forging or misrepresenting one's identity in electronic communications.

d. Concealing or masking the identity of electronic communications.

e. Sending anonymous email.

f. "Letter Bombing," (i.e., resending the same email repeatedly to one or more recipients).

g. Sending or forwarding chain letters.

h. Playing computer games during working hours.

i. Exploiting listservers or similar systems for the widespread distribution of unsolicited mail, (i.e., "spam").

j. Use of email user identification for commercial purposes.

k. Loaning or selling user identification information.

l. Using the District's computer and network resources for illegal activities. Examples of unlawful use include, but are not limited to:

- Harassment and intimidation of individuals.
- Pornography.
- Threats.
- Theft.
- Unauthorized attempts to access data.

m. Attempts to breach security measures.

n. Attempting to circumvent installed data protection methods that are designed to provide secure data and information.

o. Entry, examination, use, transfer and tampering with the accounts and files of others without proper authorization.

p. Altering email system software or hardware configurations.

q. Installing software without prior approval of MIS or knowingly running computer viruses or password cracking programs.

r. Theft or damage of equipment and software.

s. Attempting to interfere with the physical computer network/hardware.

t. Interfering with the work of others or with District or other computing facilities.

u. Using a "sniffer" or other methods in an attempt to "crack" passwords.

sniffer – a program that monitors and analyzes network traffic, which can be used legitimately or illegitimately to capture data being transmitted on a network. A router with a sniffer may be able to read other information as well as the source and destination addresses. The term "sniffer" is

also used for a program that analyzes data other than network traffic.

3. **District Email Services**
   - **a.** Email services are extended for the sole use of District employees and other appropriately authorized users to accomplish tasks related to and consistent with Northwest Fire District's mission.
   - **b.** District email systems and services are District facilities, resources and property as those terms are used in District policies and applicable law.
   - **c.** Any email address or account assigned by the District to individuals, sub-units, or functions of the District, is the property of Northwest Fire District.

4. **Authorized Email Service Restrictions.**
   - **a.** Email users are required to comply with state and federal law, Northwest Fire District policies, and normal standards of professional and personal courtesy and conduct. Access to District email services is a privilege that may be wholly or partially restricted by the District without prior notice and without the consent of the email user:
     - When required by and consistent with applicable law or policy.
     - When there is a reasonable suspicion that violations of policy or law have occurred or may occur.
     - When required to meet time dependent, critical operational needs.
   - **b.** Such access restrictions are subject to the approval of the appropriate District supervisory or management authority (e.g., department heads, systems managers, etc.). The autonomous operational units of the District shall establish or identify these authority levels.
   - **c.** If a user has been requested by another user via email or in writing to refrain from sending email messages, the recipient is prohibited from sending that user any further email messages until such time as he/she has been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this policy.
   - **d.** Northwest Fire District operational units may define additional "Conditions of Appropriate Use" for local computing and network facilities to supplement this policy with additional detail, guidelines, or restrictions. Such conditions must be consistent with and subordinate to this policy, and are intended to deal primarily with situations of limited resource supply.

e. When an individual's affiliation with the District ends, an attempt may be made to redirect email for a reasonable period of time as determined by the District for purposes consistent with this policy and the Northwest Fire District's mission. The District may elect to terminate the individual's email account or continue the account, subject to approval by appropriate District supervisory and systems operational authority.

5. Authorized Access. The District may permit the inspection or monitoring of email when:

a. Required by or consistent with applicable law or policy such as Arizona Public Records law (A.R.S. § 39-121, regarding inspection of public records); or any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on District systems to be accessed by authorized personnel in certain circumstances.

b. There is a reasonable suspicion that violations of law or District policy have occurred or may occur.

c. There are time dependent, critical operational needs of District business if the District determines that the information sought is not more readily available by other means.

NOTE: In such instances, the District will, as a courtesy, generally attempt to inform email users prior to any inspection or monitoring, except when such notification would be detrimental to an investigation of possible violation of law or District policy. Users are required to comply with District requests for access to, and copies of, email records when access is required or allowed by applicable law or policy regardless of whether such records reside on a computer housed or owned by Northwest Fire District. Failure to comply with such requests may lead to disciplinary or other legal action pursuant to applicable laws or policy, including, but not limited to appropriate District personnel policies or Codes of Conduct.

6. Preventing Inadvertent Disclosure – Display screens. The display screens for all microcomputers (PC's) workstations, and terminals used to view or process sensitive data – including personal information – should be positioned such that they cannot be viewed by people who should not have access (e.g., through a window, from an adjacent hallway, or waiting areas, etc.).

7. Expectation Of Compliance – Employees are expected to comply with laws and policies that apply to the collection or use of personal information and they are expected to take steps necessary to protect the privacy of all employees and patrons.

8. **Disclosure To Third Parties –** Disclosure of personal information about District employees or patrons is strictly prohibited, (see *Personnel Records:* 5. E. 4. d. and e. and *Confidentiality of Information:* 5. F.).
9. **Inspection Of Stored Information –** Consistent with applicable law or policy, District officials may examine records, paper files, electronic mail, disk drive file directories and files, and other information. Accordingly, such use does not carry with it a reasonable expectation of privacy. Examinations are typically performed to assure compliance with policies or law, to support the performance of internal or external investigations, to assist with the management of Northwest Fire District's information systems, to prevent abuse of resources, or to assist law enforcement.
10. **Responsibility to Report Violations –** Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate District authorities and/or law enforcement agencies. Violations may result in revocation of email service privileges; employee disciplinary action up to and including termination; referral to law enforcement agencies, or other legal action.

D. General Use Cautions

Users should be aware of the following:

1. Both the nature of email and the public character of the District's business make email less private than users may anticipate. For example, email intended for one person sometimes may be widely distributed due to the ease with which recipients can forward it to others. A reply to an email message posted on an electronic bulletin board or "listserver" intended only for the originator of the message may be distributed to all subscribers to the listerv. Furthermore, even after a user deletes an email record from a computer or email account, it may persist in whole or in part in system logs, in the directories of the person who received the message, or on the system backup tapes, which may be retained for long periods of time. All these items may be subject to disclosure under applicable law and this policy. The District cannot routinely protect users against such eventualities.
2. Email, regardless whether created, received, or stored on District equipment, may constitute an "Official Record" (as defined by A.R.S. § 41-1350); may be a "Public Record" subject to disclosure under the Arizona Records Law (A.R.S. § 39-121); or may also be subject to disclosure or access under other laws or as a result of litigation.
3. The District does not automatically comply with all requests for disclosure, but attempts to evaluate such requests against the

precise provisions of the Public Records Law or other applicable law concerning disclosure and privacy.

4. The District, in general, cannot and does not wish to be the arbiter of the contents of email. Neither can the District, in general, protect users from receiving email they may find offensive. Members of the Northwest Fire District community, however, are strongly urged to use the same personal and professional courtesies and considerations in email as they would in other forms of communication, and particularly those applicable to written communications since email creates a tangible record of that communication.

5. There is no guarantee, unless "authenticated" mail systems are in use, that email received was in fact sent by the purported sender, since it is relatively easy, although a violation of this policy, for senders to disguise their identities. Furthermore, email that is forwarded may also be modified. Authentication technology is not widely and systematically in use at Northwest Fire District as of the date of this policy. As with print documents, in case of doubt, receivers of email messages should check with the purported sender to validate authorship or authenticity.

6. Encryption of email is another emerging technology that is not in widespread use as of the date of the policy. This technology permits the encoding of email so that for all practical purposes it cannot be read by anyone who does not possess the right key. Because of Federal regulations (36 CFR 1234) and State of Arizona directives for the maintenance of email public records, encryption should not be used for storage of District email.

7. Inappropriate email use may expose the District and individual users to claims for damages through copyright infringement, libel, breach of privacy, or other personal or proprietary rights.

8. Federal law and Northwest Fire District policies regarding copyright and intellectual property apply to email. Users shall not violate others' copyrights. Unless the material is legally established as being in the public domain or unless there is explicit release by the copyright owner, employees may not copy email information. Under copyright law, individuals may or may not have copyright in email material they have created. Individuals should check with the appropriate authorities before assuming they have copyright in such material.

9. Even though an email sender and recipient have deleted their email, backup copies may exist for periods of time and in locations unknown to the recipient. These copies may be accessed or disclosed consistent with applicable policy or law.

E. Retention and Destruction of Computer Records

1. **Disposal of personal information.** When personal information is no longer needed and is not required to be maintained by law or as a Public Record, it should be disposed of in an approved manner. Suggested destruction methods and techniques for hardcopy, computer disk and media, embedded systems and other data storage systems can be acquired by contacting the MIS Administrator.
2. Thoroughly shredding or recycling or recycling in appropriate secured containers is an effective method for destroying hardcopy documents.
3. Destruction of information on computer disks and other magnetic media should be accomplished with an overwriting process. A simple "erase" process is not sufficient to completely destroy information and consequently enables inappropriate recovery and disclosure of information. Embedded hard disk drives or other data storage systems may require physical destruction.

F. Off-Site Use of Personal Information

The requirements for handling personal information are the same regardless of whether on or off District time and/or on or off District property.