

Earnhart Hill Regional Water & Sewer District

Public Records Policy

Table of Contents

Maintenance of Records.....	3
Storage of Records.....	4
Archiving of Inactive Records.....	4
Electronic Records.....	4
Destruction/Disposal of Records.....	5
Responding to Records Requests.....	5
Protection of Personal Information.....	8
Managing Electronic Mail.....	11

Maintenance of Records

As a political subdivision of the state of Ohio, the Earnhart Hill Regional Water & Sewer District is required to comply with the Ohio Public Records Law (R.C. Chapter 149). R.C. §149.351 provides:

All records are the property of the public office concerned and shall not be removed, destroyed, mutilated, transferred, or otherwise damaged or disposed of, in whole or in part, except as provided by law or under the rules adopted by the records commissions provided for under sections 149.38 to 149.42 of the Revised Code or under the records programs established by the boards of trustees of state-supported institutions of higher education under section 149.33 of the Revised Code. Such records shall be delivered by outgoing officials and employees to their successors and shall not be otherwise removed, transferred, or destroyed unlawfully.

R.C. §149.43 defines a “public record” as “any record which is kept by any public office.” R.C. §149.011(G) defines a “record” as

any document, device, or item, regardless of physical form or characteristic, including an electronic record as defined in section 1306.01 of the Revised Code, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office.

Pursuant to R.C. §6119.07, the District’s Board of Trustees is required to establish rules and regulations to provide the procedure for its actions and any other lawful subject necessary to the operation of the district and the exercise of the powers granted to the Board. Pursuant to that authority, the Board of Trustees has adopted this public records policy, which governs maintenance of the District’s records.

Storage of Records

Public Records must be stored so that they are available for inspection by the public during regular business hours. Records must be stored in a manner that they are protected from destruction, or damage which will impact their retrieval, by fire, water or other catastrophe. Where practical, records should be stored in a redundant manner so that destruction, or material damage, will not impact the District's ability to retrieve information contained within the records.

R.C. Chapter 1347 also requires that the District take "reasonable precautions to protect personal information,"¹ maintained within its records, "from unauthorized modification, destruction, use, or disclosure." For this reason, records containing "personal information" must be stored in such a way that such personal information is secure, and so that personal information contained within public records may be readily identified as personal information and so that steps may be taken to guard against unauthorized modification, destruction, use or disclosure of personal information. See, Section of this policy relating to Protection of Personal Information.

Archiving of Inactive Records

Although some records may still be within the established Retention Periods, they may not be needed on a daily basis for the operations of the District. These records would be classified as inactive records, which may be archived.

The process of archiving inactive records involves moving the records to a location, either within, or outside of, the District's offices, so as to make space available for the storage of active records. The location where records are archived must provide conditions, which ensure the safety and integrity of the archived records.

Although archived records need not be accessible on a daily basis by the District's staff, they still must be accessible within a reasonable time so that they are available for inspection by the public. When inactive records are archived, the District must maintain information as to the location of such records. Additionally, the archived records must be organized, or indexed, in such a manner as to ensure that they can be located as needed, or in response to a request for inspection.

Electronic Records

Records in electronic format should be scheduled in the same manner that paper and microfilm records are scheduled; they should be scheduled according to record series. The electronic media that the record is stored on (i.e. CD,

¹ "Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person. R.C. §1347.01(E).

magnetic tape, etc.) is simply storage media, not a record series. Electronic records include, but are not limited to, such records as:

- Databases
- E-Mail
- Web pages
- Electronic Images
- Digitally-stored voice messages

A major issue related to electronic records is the handling of e-mail messages. An e-mail message is a document or item created or received by a public office. Whether the e-mail serves to document the organization, functions, policies, decisions, procedures, operations or other activities is the deciding factor as to its status as a record. This is true of any communication, whether electronic or paper. The District's E-Mail Policy is attached to this manual, as Appendix A.

Destruction/Disposal of Records

1. The District is currently creating a records inventory and retention schedule. No records of the District can be destroyed until the retention schedule has been approved by the Ohio Historical Society and a Records Policy Manual, which this policy will become a part thereof, has been approved by the Board of Trustees.

Responding to Records Requests

Upon request, the District is required, by R.C. §149.43(B)(1), to make copies of public records available, at cost, within a reasonable period of time. To meet this duty, the following policies shall apply to each such response:

1. All requests to inspect, and/or receive copies of, the District's public records shall be referred to the District's Records Officer, or in the event of his/her unavailability, to the General Manager.
2. Whenever possible, a response to a records request shall be provided on the same business day as the request is received.
3. The District is only required to provide copies of records that it actually maintains. The District is **not** required to produce special reports, or data compilations, in a form that is not regularly maintained by the District. However, if requested information may be extracted from a database, or other records storage system, through the use of an available, or readily structured, query, it must be produced in the format requested.
4. If the employee receiving the request is unclear as to the scope of the request, he/she may ask the requester to further explain what type of information the requester is seeking to assist the District in determining what records would be responsive to the request. A requester's decision to refuse to further explain the request shall not, in and of itself, be a reason to refuse to comply with the request.

5. If a requester makes an ambiguous or overly broad request or has difficulty in making a request for copies or inspection of public records such that District cannot reasonably identify what public records are being requested, the District may deny the request but shall provide the requester with an opportunity to revise the request by informing the requester of the manner in which records are maintained by the District and accessed in the ordinary course of the District's duties.
6. Unless specifically required or authorized by state or federal law, the District may NOT limit or condition the availability of public records by requiring disclosure of the requester's identity or the intended use of the requested public record. Any requirement that the requester disclose the requestor's identity or the intended use of the requested public record constitutes a denial of the request.
 - a. The District may ask a requester to make the request in writing, may ask for the requester's identity, and may inquire about the intended use of the information requested, but may do so only after disclosing to the requester that a written request is not mandatory and that the requester may decline to reveal the requester's identity or the intended use and when a written request or disclosure of the identity or intended use would benefit the requester by enhancing the ability of the public District to identify, locate, or deliver the public records sought by the requester.
 - b. The District should ask that the requester provide a mailing address, or an email address, only if the requester desires that copies of records be delivered by mail, or by electronic transmission.
 - c. If the requester declines to make a written request, the District employee receiving the oral request shall create a written record of his/her understanding of the scope of the request; such record should, at a minimum, describe the record(s) requested and the time period covered by the request. A copy of the employee's written record of his/her understanding of the request should be immediately provided to the requester.
7. Some records kept by the District may be outside of the statutory definition of public records. Examples include:
 - a. Social security numbers, tax identification numbers, addresses, dates of birth or other personal information, contained in records relating to District employees, contractors, vendors or customers.
 - b. Personal financial information (such as credit card, and bank account, information) contained in records relating to District employees, contractors, vendors or customers.
 - c. Personally identifiable health information contained in records relating to District employees.
 - d. Records containing information relating to security procedures for the District's facilities.

e. Records protected by attorney-client privilege

Some of these types of information may be contained within a record that is, itself, a public record. If a public record contains information that is exempt from the duty to permit public inspection or to copy the public record, the District is required to make available all of the information within the public record that is not exempt. When making that public record available for public inspection or copying that public record, the District shall notify the requester of any redaction or make the redaction plainly visible. A redaction shall be deemed a denial of a request to inspect or copy the redacted information, except if federal or state law authorizes or requires a public office to make the redaction.

8. In the event the employee receiving a public records request is unsure whether information should be made available to the requester, the employee should request that the General Manager review the request; however, the review process (which may include consultation with the District's legal counsel) should not usually delay the response to the request by more than three (3) business days. If a request is ultimately denied, in part or in whole, the District shall provide the requester with an explanation, including legal authority, setting forth why the request was denied. If the initial request was provided in writing, the explanation also shall be provided to the requester in writing.
9. The person making a public records request has the right to choose to have the public record duplicated upon paper, upon the same medium upon which the District keeps it, or upon any other medium upon which the General Manager determines that the record reasonably can be duplicated as an integral part of the normal operations of the District. Although copies of most District records can be provided on paper, copies of records maintained in an electronic format can also be provided on either a compact disc (CD) or a floppy disk, or as an e-mail attachment; however, a requester should be cautioned that some of these records might not be readable in such electronic format without special software.
10. Copies of public records shall be provided upon request at the District's actual cost. For purposes of this policy, "actual cost" includes the cost of depleted supplies, records storage media costs, actual mailing and alternative delivery costs, or other transmitting costs, and any direct equipment operating and maintenance costs, including actual costs paid to private contractors for copying services. The time spent by the District's employees in assembling the copies shall not be included in the cost of providing the copies.
 - a. Paper photocopies of public records will be provided at a cost of 5¢ per page.
 - b. Copies provided on an electronic media will be provided at the District's media cost.

- c. A person who requests to receive a copy of public records shall pay in advance the estimated cost involved in providing the copy of the public record in accordance with the choice of media made by the person seeking the copy, and shall pay any additional cost prior to delivery of the copies of the public records.
11. Copies of public records will be transmitted either by U.S. Mail, courier, electronic delivery or other reasonably available method of delivery specified by the requester. The person requesting such copies shall pay in advance the cost of postage if the copy is transmitted by United States mail or the cost of delivery if the copy is transmitted other than by United States mail, and the costs incurred by the District for other supplies used in the mailing, delivery, or transmission. The District will not transmit by U.S. Mail copies of public records to, or on behalf of, the same person, or entity, more than ten (10) times per month unless the requester certifies to the District in writing that the requester does not intend to use or forward the requested records, or the information contained in them, for commercial purposes. For purposes of this provision, the term "commercial" shall be narrowly construed and does not include reporting or gathering news, reporting or gathering information to assist citizen oversight or understanding of the operation or activities of government, or nonprofit educational research.
12. The person/entity making a request to inspect, and/or receive copies of, public records request shall NOT be permitted to make copies of the public records.
13. A copy of this public records policy shall be posted on the District's internet website at www.ehrwsd.org , and shall be readily available for public review at the District's administrative offices and at each of its treatment plants. A poster shall be conspicuously displayed at each of those facilities indicating that a copy of the District's public records policy is available upon request, or at www.ehrwsd.org. A copy of this public records policy shall also be provided, or made readily available, to each employee of the District.

Protection of Personal Information

Pursuant to R.C. §1347.05, the District is required to

1. Monitor the accuracy, relevance, timeliness, and completeness of the personal information maintained within a personal information system, and, to maintain the personal information in the system with the accuracy, relevance, timeliness, and completeness that is necessary to assure fairness in any determination made with respect to a person on the basis of the information.
2. Collect, maintain, and use only personal information that is necessary and relevant to the functions that the District is required or authorized to perform by statute, or by regulation established by the Board of Trustees, and to eliminate personal information from the system when it is no longer necessary and relevant to those functions.

3. Inform a person who is asked to supply personal information for a personal information system whether the person is legally required to, or may refuse to, supply the information.
4. Take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use, or disclosure. However, these duties do not limit the District's duty to maintain, and allow the inspection of, its public records as required by R.C. §149.43.

"Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person. Although much of the personal information maintained by the District is also a public record, the following types of information are outside of the statutory definition of the term public record and shall not be used or disclosed except for the specific purposes for which it was collected:

1. Social security numbers, and tax identification numbers, contained in records relating to District employees, contractors, vendors or customers.
2. Personal financial information (such as credit card, and bank account, information) contained in records relating to District employees, contractors, vendors or customers.
3. Personally identifiable health information contained in records relating to District employees.

To the extent possible, the foregoing information shall be maintained separately from the public records of the District to protect against its unauthorized use or disclosure.

Any employee of the District who uses, or participates in the use of, personal information in an unauthorized manner, or who discloses, or participates in the disclosure of, personal information to unauthorized persons or entities, shall be subject to discipline, including reprimand, suspension or termination, at the discretion of the General Manager.

Not later than June 1, 2008, each existing employee of the District shall receive a written notice advising him/her of the right to review personal information maintained by the District that relates to him/her, and of his/her right to contest the accuracy, relevance, timeliness, and completeness of any of such information. A similar written notice shall be provided to each new employee upon commencement of his/her employment.

The General Manager shall be directly responsible for the District's personal information system(s). Not less than biennially, the General Manager, or his/her designee(s), shall review the types of personal information collected, and maintained, by the District to determine whether such information is necessary and relevant to the functions that the District is required or authorized to perform by statute, or by regulation established by the Board of Trustees, and to determine whether any such personal information should be eliminated from the system when it is no longer necessary and relevant to those functions. The General Manager shall also

determine what personal information collected by the District shall be designated as mandatory, and what personal information, if any, shall be designated as optional. Any form, or other method of collecting personal information, shall clearly disclose which information is mandatory, and which information, if any, is optional.

APPENDIX "A"

Managing Electronic Mail

Intent and Purpose

The intent of this policy is to provide and explain requirements, guidelines and best practices for electronic mail (e-mail) messages that meet the criteria for records as defined by the Ohio Revised Code.

These guidelines have a two-fold purpose. First, they are intended to assist District employees in complying in their use of e-mail with Ohio public records law. Second, the guidelines promote best practices and suggestions that facilitate the effective capture, management, and retention of electronic messages as public records.

Introduction

Electronic mail systems, commonly called e-mail, are becoming the communications method of choice for many District employees. E-mail messages are often used as communication substitutes for the telephone as well as to communicate substantive information previously committed to paper and transmitted by more traditional methods. This combination of communication and record creation/keeping has created ambiguities on the status of e-mail messages as records.

The management of e-mail systems touches on nearly all functions for which the District is dependent on recordkeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly, then, is the same as for other records keeping systems -- to ensure compliance with Ohio laws concerning the creation of, retention of, and access to public records.

District employees must be made aware that e-mail messages, like paper records, must be retained and destroyed according to established records management procedures. The District's e-mail system should be set up or modified to facilitate electronic records management. Procedures and system configurations will vary over time according to the District's needs and the particular hardware and software in place.

Definitions

E-mail systems are store-and-deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that shuffles messages to users within an agency or office; to a wide area network e-mail system which carries messages to various users in various physical locations; to Internet e-mail that allows users to send and receive messages from other Internet users around the world.

E-mail messages are electronic documents created and sent or received by a computer system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

Legal Requirements

The Ohio Revised Code (ORC) includes no specific definition for electronic mail, however ORC Section 149.011(G) provides the following definition:

"Records" includes any document, device, or item, regardless of physical form or characteristic, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office.

Clearly, an e-mail message is a document or item created or received by a public office. Whether the e-mail serves to document the organization, functions, policies, decisions, procedures, operations or other activities is the deciding factor as to its status as a record. This is true of any communication, whether electronic or paper.

E-mail messages that meet the criteria of the definition of a record must be scheduled and retained for the appropriate time period before disposition. Scheduling e-mail is discussed in detail below.

E-mail messages that meet the criteria of the definition of a record may be considered public records and must be available to the public. A record must meet the definition of a public record as defined in the Ohio Revised Code. This definition is found in Section 149.43, which states in part:

Public record means any record that is kept by any public office, including, but not limited to, state, county, city, village, township, and school district units, except that public record does not mean any of the following: medical records...

All public records shall be promptly prepared and made available for inspection to any person at all reasonable times during regular business hours. Subject to division (B)(4) of this section, upon request, a public office or person responsible for public records shall make copies available at cost, within a reasonable period of time. In order to facilitate broader access to public records, public offices shall maintain public records in such a manner that they can be made available for inspection in accordance with this division.

As with any format, an e-mail message is considered a public record unless it falls under one of the exceptions listed in R.C. §149.43. These records must be maintained and made accessible to the public upon request through the appropriate retention period.

Retention and Scheduling Requirements

E-mail itself is not considered a record series or category. It is a means of transmission of messages or information. Like paper or microfilm, e-mail is the medium by which this type of record is transmitted. Just as an agency cannot schedule all paper or microfilm records together under a single retention period, an agency cannot simply schedule e-mail as a record series. Rather, retention or disposition of e-mail messages must be related to the information they contain or the

purpose they serve. The content, transactional information, and any attachments associated with the message are considered a record (if they meet the ORC criteria). The content of e-mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

Simply backing up the e-mail system onto tapes or other media or purging all messages after a set amount of time are not appropriate strategies for managing e-mail.

For the purposes of this document, there are four categories of e-mail retention: non-record messages, transitory messages, intermediate messages, and permanent messages.

Non-Record Materials: E-mail messages that do not meet the criteria of the Ohio Revised Code definition of a record may be deleted at any time, unless they become part of some official record as a result of special circumstances. These types of messages may include:

Personal Correspondence: Any e-mail not received or created in the course of District business, may be deleted immediately, since it is not an official record: the "Let's do lunch" (not a State-business lunch) or "Can I catch a ride home" type of note.

Non-District Publications: Publications, promotional material from vendors, and similar materials that are "publicly available" to anyone, are not official records unless specifically incorporated into other official records. In the electronic world, this includes listserve messages (other than those you post in your official capacity), unsolicited promotional material ("spam"), files copied or downloaded from Internet sites, etc. These items may be immediately deleted, or maintained in a "Non-Record" mail box and deleted later, just as you might trash the unwanted publication or promotional flyer. However, for example, if you justify the purchase of a "Zippo Filing System" by incorporating the reviews you saved (from the "Files R Us Listserv") in your proposal to your boss, those listserv messages become official records and must be retained in accordance with the retention schedule for purchasing proposals.

Official Records -- Retain As Required

E-mail messages that meet the definition of a record in the ORC are official records and must be scheduled, retained and disposed of as such. These official records fall into the following categories:

Transient Retention: Much of the communication via e-mail has a very limited administrative value. For instance, an e-mail message notifying employees of an upcoming meeting would only have value until the meeting has been attended or the employee receiving the message has marked the date and time in his/her calendar.

Transitory messages do not set policy, establish guidelines or procedures, certify a transaction or become a receipt. The informal tone of transitory messages might be compared to a communication that might take place during a telephone conversation or conversation in an office hallway. These

types of records, which include telephone messages, drafts and other limited documents which serve to convey information of temporary importance in lieu of oral communication, are transient documents and should be retained until no longer of administrative value, and then destroyed.

Intermediate Retention: E-mail messages that have more significant administrative, legal and/or fiscal value but are not scheduled as transient or permanent should be categorized under other appropriate record series. These may include (but are not limited to):

General Correspondence: Includes internal correspondence (letters, memos); also, correspondence from various individuals, companies, and organizations requesting information pertaining to agency and legal interpretations and other miscellaneous inquiries. This correspondence is informative (it does not attempt to influence agency policy). Retention: 1 year, then destroy

Routine Correspondence: Referral letters, requests for routine information or publications provided to the public by agency which are answered by standard form letters. Retention: 6 months, then destroy

Monthly and Weekly Reports: Document status of on-going projects and issues; advise supervisors of various events and issues. Retention: Retain 1 year, then destroy

Minutes of Staff Meetings: Minutes and supporting records documenting internal policy decisions. Retention: Retain 2 years, then destroy.

Permanent Retention: E-mail messages that have significant administrative, legal and/or fiscal value and are scheduled as permanent also should be categorized under the appropriate record series. These may include (but are not limited to):

Executive Correspondence: Correspondence of the General Manager, or Assistant General Manager, dealing with significant aspects of the administration of the District. Correspondence includes information concerning District policies, program, fiscal and personnel matters. Retention: 2 years, then transfer to District's permanent archives.

Departmental Policies and Procedures: Includes published reports, unpublished substantive reports and policy studies. Retention: Retain until superseded, obsolete or replaced, then transfer to the District's permanent archives for their possible retention or destruction.

Not all e-mail messages will fall into the foregoing record series. In the case of confusion as to the proper record series, an employee should consult the District's Records Manager.

Guidelines and Best Practices for Managing E-mail

Record Copy E-mail

E-mail users should be aware that e-mail messages are often widely distributed to a number of various recipients. Determining which individual maintains the record copy of the message, *i.e.* the original message that must be retained per the retention schedule, is vital to e-mail management. If the holder of the record copy is not identified and aware of his/her responsibility, the District may find that no one retains the message or that everyone retains the message. Neither of these scenarios is appropriate.

For example, agency policy documents which are transmitted to multiple recipients via an e-mail system need not be maintained by each recipient beyond his or her need for this information if record copy responsibility is established so that the record is maintained by some office or agent for its established retention period. In this example, a logical record copy responsibility rests with the creator of the policy document. Prompt deletion of duplicate copies of e-mail messages from an e-mail system makes the system as a whole much easier to manage and reduces disk space consumed by redundant information.

Generally speaking, the individual who sends an e-mail message should maintain the record copy of the message. However, the varied uses and wide distribution of e-mail may result in many exceptions to this rule that will have to be dealt with internally.

Filing

Non-transitory e-mail messages should be filed in a way that enhances their accessibility and that facilitates records management tasks. The District's e-mail system should set up or modified to facilitate records management and appropriate filing systems. Procedures and systems configurations will vary over time according to the District's needs and the particular hardware and software in use.

In addition to the IN and OUT boxes that come with the mail system, employees have the option of creating other "mailboxes" or "folders." After brief periods in an employee's IN-OUT boxes, messages should be transferred to other folders, based on business and retention requirements.

Employees are responsible for classifying messages they send or receive according to content, the District's folder/directory structure and established records series.

Distribution Lists

If an employee sends a message, or messages, to a "distribution list" (not a listserve, but a specified list of individuals), the employee must also keep a copy of the members of that list for as long as the employee is required to keep the message itself. It is of little value to know that the "Security Alert!" notice went to "Swat Team 7," without knowing whether Arnold S. received the message. Nicknames present a similar problem.

Subject Lines

An employee should fill in the subject line on an e-mail both to help the recipient identify and file messages, and to help the employee file OUT box messages that must be retained for some period. Subject lines should be as descriptive as possible.

Storage of E-mail

Although e-mail records may be stored in a variety of ways, most messages should simply be stored on-line by individual employees. However, if the capability is developed to provide for centralized on-line storage, a back-up system should be developed for such central store. In the event of centralized storage, procedures must be developed to catalogue, or index, individual messages in a manner which will permit compliance with retention/disposal requirements; such procedures must also apply to any back-up system.

E-mail Messages and the Rules of Evidence

The Records Manager, in consultation with the District's legal counsel, should become familiar with both state and federal "rules of evidence" requirements. For records maintained in electronic information systems, including e-mail systems, courts concentrate on assurances that records, and the systems in which the records are created and maintained, are reliable. The reliability of the process or system used to produce records, not the type of media or technology used, determines the admissibility of records in evidence. Moreover, the federal rules of evidence place the burden for the identification of relevant records on the record creator, and often within a ninety-day time period. At a minimum, agency personnel should ensure the following:

- e-mail systems used to create, receive and maintain e-mail messages have full, complete, and up-to-date systems documentation
- e-mail systems follow all recommendations for system security
- complete systems backups are regularly and consistently performed
- e-mail system retains all data and audit trails necessary to prove its reliability as part of the normal course of agency business
- the record copy of a message is identified and maintained appropriately
- backup procedures should be coordinated with disposition actions so that no copies of records are maintained after the retention period for the records has expired

Again, the Records Manager must plan for records maintenance and record copy responsibilities for the records system to meet requirements for reliability and legal records disposition. The e-mail system should allow the server administrator to prevent destruction of records for legal and/or audit purposes.

Access

A major challenge for the District is to guarantee that records maintained in electronic information systems are accessible and usable for the entire length of

the retention period. Rapid changes and enhancements to both hardware and software compound this challenge. As many e-mail systems have limitations in storage space that cause operational problems when messages are stored in the system beyond a specific period (such as sixty or ninety days), procedures must be in place to transfer records from the e-mail system to another electronic records keeping system to meet retention requirements.

Messages should be maintained in a format that preserves contextual information (metadata) and that facilitates retrieval and access. The system should allow deletion of messages once their retention periods expire.

Beyond this generic challenge of technology change, there are more mundane, but equally critical steps that must be in place to ensure that records created by e-mail systems can be located and retrieved when required. A central step is a system of standardized naming conventions and filing rules within the e-mail systems.

E-mail messages should be indexed in an organized and consistent pattern reflecting the ways in which records are used and referenced. Records maintained electronically, including e-mail messages, have an advantage over conventional "hard copy" document filing systems in that indexing for multiple access points is relatively simple and inexpensive, provided an effective indexing framework is in place. Planning records indexing and retrieval points is time well spent. Unnecessary time needed to retrieve electronic records is not productive staff time, and is an annoyance to the public as well. Messages should be stored in a logical filing system that is searchable by multiple data elements.

Responsibility

Although the Records Manager has the ultimate responsibility for ensuring the compliance of the e-mail system with this policy, all employees must understand and carry out their role in the records management process. The Records Manager must work with the District's IT Manager to manage and modify the District's e-mail system(s) to meet the requirements of this policy, and the needs of the District. The Records Manager must also provide ongoing training and support to all employees so that the employees understand, and properly perform, their responsibilities under this policy. Unauthorized users should not be able to access, modify, destroy or distribute records.