Electronic Records Management Guidelines

Contents

Section 1: Authority

These Guidelines are hereby jointly issued by the Supervisor of Records, the Records Conservation Board and the Information Technology Division under the authority of G. L. c. 66, § 1; G. L. c. 30, § 42; and G. L. c. 110G, § 17.

Section 2: Purpose and Scope

Purpose The purpose of these Guidelines is to help ensure that government electronic records are created, maintained, disseminated and destroyed in a manner consistent with the transparency and accountability requirements of the Massachusetts Public Records Law, G. L. c. 66, § 1, et seq. and the standards set by the Records Conservation Board.

While many concerns are the same as those that exist with other, more traditional forms of public records, the prevalence of electronic records raises some new issues. Therefore, government records custodians must be mindful of how business, technical and legal standards apply to electronic records.

Scope It is the responsibility of government officers who create, receive and maintain public records to ensure their safekeeping and availability to the public.

These Guidelines are intended to provide actionable ***recommendations*** to all entities subject to the provisions set by the Records Conservation Board in applying the requirements surrounding management of public records to the unique aspect of electronic records as defined by the Uniform Electronic Transactions Act, in addition to information systems, regardless of format or location.

These Guidelines are not intended to supersede, overwrite, establish policy or otherwise change any existing legal, statutory or other requirement that may apply to government data, information systems or records of any other nature.

For purposes of these Guidelines, electronic records include, but are not limited to, records created, generated, sent, communicated, received, or stored by electronic means.

Section 3: Records Custodian Responsibilities

Each officer in charge of a government office or department is the custodian of the records held by that office or department and therefore is responsible for managing the entity's electronic records.

It is advised that Records Custodians adopt and implement a formal **Electronic Records Management Program** that, at a minimum, incorporates the following elements:

Administrative Management

(1) Assignment of the responsibility to develop and implement a program for the management of all records created, received, maintained, used, or stored on electronic media;

(2) Establishment of formal procedures that address records management requirements, including recordkeeping requirements and disposition;

(3) Method, controls or mechanisms for addressing electronic records that are exempt from disclosure under G. L. c. 4, § 7(26), or any other applicable statute;

(4) Establishment of procedures that will reasonably ensure that the provisions of these Guidelines are applied to electronic records that are created or maintained by contractors or other agents;

(5) Establishment of procedures that require departing public entity officials, employees, and other agents return or destroy, as appropriate, all portable storage media or any other device capable of storing data in said individual's possession that may contain the public entity's electronic records;

(6) Preventative controls to ensure that no public entity electronic records are copied or transferred by or on behalf of the departing individual or agent without supervisory review to make certain that such copying or transfer will not violate records retention, confidentiality or security requirements and ensures compliance with G. L. c. 66, § 14;

(7) Validation that new electronic information systems or enhancements to existing systems support established Electronic Records Management Program requirements and associated Procedures;

(8) Integration and alignment of the management of electronic records with other records and information resources management programs of the public entity and of any over-arching authority's programs;

(9) Compliance with all policies, procedures, and standards such as those issued by the Supervisor of Records; the Records Conservation Board; and, with respect to the Executive Department, those issued by ITD as Policies, Standards and Procedures; or other offices empowered to regulate electronic records as well as any other applicable laws or statutes;

(10) Review of electronic information systems for conformance to established agency procedures, standards, and policies as part of a periodic review, which should include an assessment of whether the records have been properly identified and described, and

whether the schedule descriptions and retention periods reflect the current informational content and use;

Notification & Education Elements

(11) Written notification to the Supervisor of Records (Form RMU-4) and Records Conservation Board (Form RCB-4) of the name and title of the person assigned the responsibility of managing electronic records;

(12) Incorporation of the electronic records management program's objectives, responsibilities, and authorities in pertinent agency directives and dissemination of the directives throughout the entity as appropriate;

(13) Establishment of a program that encourages and supports work in conjunction with the Records Conservation Board to ensure compliance with the Statewide Records Retention Schedule by:

a. Developing and maintaining appropriate records disposition practices;

b. Securing the Records Conservation Board's approval of records disposition schedules; and

c. Validating the implementation of the Record Conservation Board's provisions.

(14) Ensures that adequate training is provided on meeting the requirements of an entity's electronic records management program for:

a. End -users of electronic mail systems, websites, social media and desktop documents on recordkeeping requirements, and moving or copying records for inclusion in an agency recordkeeping system; and,

b. Users who have control of electronic information systems or in the operation, care, and handling of the equipment, software, and media used in the system.

Documentation

(15) Development and maintenance of up-to-date documentation about all electronic information systems that will allow entities to:

a. Specify all technical characteristics necessary for reading or processing the records;

b. Identify all defined inputs and outputs of the system;

c. Define the contents of the files and records;

d. Determine restrictions on access and use;

e. Understand the purpose(s) and function(s) of the system;

f. Describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and

g. Ensure the timely, authorized disposition of the records;

(16) Specification of the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements, and maintenance of inventories of electronic information systems to facilitate disposition; periodic

refreshment of media on which electronic records are stored to ensure against media degradation and loss of interoperability with current information technology systems.

Section 4: Information Systems that produce, use or store Electronic Records

The Records Conservation Board and the Supervisor of Records require some assurances from agencies that their record-keeping systems produce accurate, secure, and reliable records. Agencies must be able to demonstrate consistent, controlled data handling during the active and inactive life of the data.

In order to comply with existing requirements, it is advised that entities that utilize electronic information systems to produce, use or store data files address the following:

System Design

(1) Incorporate disposition instructions for the data into the system's design.

Note: Systems that are subject to G. L. c. 93I must adhere to the special disposition rules pertaining to personal information as identified in that statute.

(2) Require manual commands entered by agency personnel to approve disposition of identified records. This will help to prevent inadvertent disposition that is likely when systems rely solely on automated, age-based disposition of electronic records.

System Documentation

(3) Develop and maintain adequate and up-to-date technical documentation for each electronic information system that produces, uses, or stores data files. It is recommended that to comply with current minimum documentation requirements, entities include a narrative description of the system comprised of:

(a) The physical and technical characteristics of the records, including a record layout that describes each field, including its name, size, starting or relative position, and a description of the form of the data, such as alphabetic, zoned decimal, packed decimal, or numeric, or a data dictionary, or the equivalent information associated with a data base management system, including a description of the relationship between data elements in data bases; and,

(b) Any other technical information needed to read or process the records.

Electronic recordkeeping systems that maintain the official file copy of a record

(4) Prior to being used to maintain official file copies, electronic recordkeeping systems should:

(a) Support provisioning that allows all authorized users of the system to retrieve desired documents, such as an indexing or text search system;

(b) Enforce an appropriate level of security to ensure the integrity of the documents;

Note: Executive Department agency systems must meet ITD's security policies and standards.

(c) Ensure that a standard interchange format is provided, when necessary, to permit the exchange of documents on electronic media between agency computers using

different software/operating systems and the conversion or migration of documents on electronic media from one system to another;

(d) Address disposition of documents in accordance to these guidelines and overarching regulations, including, when necessary, the requirements for transferring permanent records to the State Archives facility or other facility for the safekeeping of permanent records;

(e) Maintain sufficient information to allow for identification of each document within a given electronic information system. Identifying information should include: office of origin; file code; key words for retrieval; addressee, if any; signatory; author; date; authorized disposition, coded or otherwise; and security classification, if applicable; and,

(f) Correlate official file copies maintained in electronic recordkeeping systems with related records on paper, microform, or other media as appropriate.

Website-Related Documents

Public entities are advised that records created or posted to websites, including externally hosted websites, are subject to the same electronic records requirements as records created or maintained on internal, non-web-based electronic recordkeeping system. Therefore, public entities need to ensure:

(5) Retention of technical documentation of the design, construction, and use of the website, including a general description of the site's purpose, descriptions of major features and sections, diagrams and descriptive lists of links, descriptions of data sources, periodic screen dumps of major pages and electronic snapshots of web pages;

(6) Websites that offer users transactional opportunities are able to retain and provide access to all data related to such transactions. Examples of transactional opportunities may include but are not limited to: submission of payments, applications or other on-line business.

Social Media Records

Public entities that use social media should be aware that social media sites contain communications sent to or received by state employees that are subject the same electronic records requirements discussed throughout these Guidelines.

Note: Public entities that use social media should be aware that most social media sites are hosted by third party providers. Consequently, the physical hardware and software that enable the social media site are located at, and under the control of, an entity other than the Commonwealth. Therefore, public entities have limited control over the functionality or business practices offered by such sites and the legal terms to which they are subject. These terms may impact adequacy of accessibility for people with disabilities, documentation, recordkeeping requirements, records management responsibilities, and records disposition. Public entities should be aware that the social media provider is unlikely to change features and functionality that do not meet all of the public entity's recordkeeping and records management obligations.

Therefore, public entities need to ensure procedures are implemented to allow for:

(7) Review of third party social media service provider's terms of service for its records retention practices.

Note: While third party social media providers will most likely save the public entity's content for some period of time, they generally will not save it indefinitely.

(8) Retention of a copy of the social media content in accordance with the Statewide Records Retention Schedule.

Note: To the extent that the social media provider's policies are inconsistent with the Statewide Records Retention Schedule, the public entity is obligated to take affirmative steps to retain copies of social media posts, such as taking a periodic screenshot of the social media sites in order to meet their agency's records retention obligations.

Desktop Documents

In order to ensure compliance with existing requirements, public entities need to ensure procedures are implemented that address the following unique aspects of records created or received through desktop applications such as Microsoft Office and Open Office.

(9) Ensure that word-processing, spreadsheet, presentation, task list, contact, calendar and other desktop documents are identified, preserved and disposed of in a manner consistent with the Statewide Records Retention Schedule;

(10) Identify and capture desktop documents created and received by employees in remote locations or on external devices, such as in the field or employee home offices, portable devices, such as tablets, notebooks, laptops, personal digital assistants and portable storage devices.

Section 5: Electronic Mail Message Records

In Massachusetts, the term "public record" is broadly defined to include all documentary materials or data created or received by any officer or employee of any governmental unit, regardless of physical form or characteristics, unless it falls under one of the statutory exemptions to the Public Records Law. G. L. c. 4, § 7(26). Consequently, email is subject to the disclosure, retention, and maintenance provisions as required by law. G. L. c. 66.

To be compliant with existing regulations, public entities need to address the following unique aspects of electronic mail:

Preservation of Transmission Data

(1) The Statewide Records Retention Schedule requires that public entities retain specific information for each electronic mail message including:

(a) The names of the sender and addressee(s), including addressees who are cc'd to an electronic mail message;

(b) The date the message was sent;

(c) Message metadata;

(d) Any attachment to the electronic mail message must be preserved in order for the context of the message to be understood; and

(e) Any other transmission data that is necessary for the purpose of providing the context of the record.

(2) If an electronic mail system identifies users by codes or nicknames, or identifies addressees only by the name of a distribution list, names on directories or distributions lists should be retained to ensure accurate identification of the sender and addressee(s) of messages that are records.

(3) Provide instructions to electronic mail message users specifying when to request receipts or acknowledgments that indicate that a message has reached a recipient's mailbox that it has been opened for recordkeeping purposes and how to preserve them in electronic mail systems that support such functionality.

(4) Public entity records sent or received using an external electronic mail system should ensure that these records are preserved in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the public entity for recordkeeping purposes.

Additional Consideration for Proper Maintenance of Electronic Mail Messages

(5) Public entities should develop procedures for the maintenance of electronic mail records in any recordkeeping systems, regardless of format, that accomplish the following:

(a) Provide for the grouping of related records into classifications according to the nature of the business purposes the records serve;

(b) Permit easy and timely retrieval of both individual records and files, or other groupings of related records;

(c) Recognize that draft documents circulated on electronic mail systems are considered to be records;

(d) Retain the records in an accessible format for their required retention period as specified by a Records Conservation Board or Supervisor of Records approved records schedule;

(e) Be easily obtained by agency employees, agents, or those properly authorized by the agency who have a business need for information in the system;

(f) Preserve all transmission and receipt data as specified in **Section 5.1.** above; and

(g) Permit transfer of permanent records to the State Archives facility or other State authorized permanent storage facility.

(6) Public entities are prohibited from using any electronic mail system to store the recordkeeping copy of electronic mail messages unless that system has all of the features specified in this section **(Section 5)** of these Guidelines.

(7) Public entities that maintain their electronic mail records in an electronic format in systems that are different from their electronic mail system must ensure that the recordkeeping system does meet all of the requirements in this section (**Section 5)** of these Guidelines. Records may be retained in an off-line electronic storage format, such as optical disk or magnetic tape.

(8) If the electronic mail system is not designed or sufficiently able to be a recordkeeping system, public entities must instruct staff on how to copy the public entity's records from the electronic mail system to a suitable recordkeeping system.

(9) Public entities that retain permanent electronic mail records scheduled for transfer to the State Archives or other permanent record storage facility must store the permanent electronic mail records in a format, and on a medium, that conforms to the transfer requirements or maintain the ability to convert the records to a required format and medium at the time transfer is scheduled.

(10) Public entities that are unable to maintain their electronic records in an electronic format and maintain paper files as their recordkeeping system must print their electronic mail records and any related transmission and receipt data, except for those that they are permitted to delete pursuant to the Statewide Records Retention Schedule.

(11) All public officials, employees and agents are responsible for maintaining their electronic mail records in accordance with the electronic mail retention policies prescribed by their respective public entities and all applicable laws and regulations. The Executive Department agencies must maintain electronic mail records in the manner specified in the Executive Office Email Retention Policy and Procedure.

Section 6: Admissibility of Electronic Records

Pursuant to G. L. c. 110G, the Uniform Electronic Transactions Act, and cognate provisions of Federal law, where the validity of electronic records is not in question, electronic records should be admissible to the same extent as paper records.

While these Guidelines do not serve to supersede any pre-existing or forthcoming rules concerning the admissibility of records, adherence to these Guidelines may enhance the presumption of the validity of electronic records maintained by a public entity.

Records custodians should be familiar with the requirements of state and federal law regarding e-discovery and should ensure that electronic records subject to discovery are captured and preserved in accordance with such requirements.

Pursuant to G. L. c. 233, § 79E, electronic records may be admitted in evidence for use in court proceedings if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it.

The suggestions contained in this section are intended to offer guidance for how to demonstrate trustworthiness.

Note: Rules of evidence involving electronic evidence is within the sole purview of the courts. Agencies should implement the following procedures or adapt existing procedures according to the guidance below to increase the likelihood of the legal admissibility of electronic records:

(1) Documentation that shows that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

(2) Demonstrable security procedures that prevent unauthorized addition, modification or deletion of a record and ensure system protection against such problems as power interruptions or natural disasters.

(3) Identification of electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the Records Conservation Board approved disposition process for all state records.

(4) Coordination of the measures in parts (1)-(3) of this Section with legal counsel, Records Liaison personnel and records management staff.

Section 7: Security of Electronic Records

Security should aim to minimize unauthorized addition, modification, alteration, erasure, or deletion of data, records, and documents. It should ensure that only authorized personnel have access to records.

In order to ensure compliance with the existing requirements, public entities need to ensure procedures are implemented that achieve the following security goals:

(1) Ensure that only authorized personnel have access to electronic records;

(2) Backup and recovery of records to protect against information loss;

(3) Personnel are trained in how to safeguard sensitive or classified electronic records;

(4) Minimized risk of unauthorized alteration or erasure of electronic records;

(5) Ensure that electronic records security is included in computer systems security plans;

(6) Comply with requirements of Executive Order 504 and the ITD Security Policies and Standards, if mandated.

Section 8: Selection and Maintenance of Electronic Records Storage Media

Agencies must be able to demonstrate consistent, controlled data handling during the active and inactive life of the data.

In order to achieve compliance with the existing requirements, public entities need to ensure that storage devices and systems for storing any regulated public entity records throughout the state's records retention lifecycle, meet the following requirements:

(1) Permit easy retrieval in a timely fashion;

  (a) Utilize a formal process or procedure to implement external labeling to facilitate identification and retrieval of stored information;

  (b) Distinguish clearly between record and non-record material;

(2) Retain the records in an accessible format until their authorized disposition date in accordance with **Section 9**;

  (a) Avoid the use of floppy disks or other forms of magnetic media not specifically designed for purposes of long term storage for the exclusive long-term storage of permanent or unscheduled electronic records;

  (b) Ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the public entity's current hardware and software. Before conversion to a different medium, public entities must determine that the authorized disposition of the electronic records can be implemented after conversion;

  (c) Prohibit smoking and eating in all areas that contain permanent or unscheduled records;

(d) Back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records should be maintained in storage areas separate from the location of the records that have been copied;

(e) Maintenance of magnetic computer tape;

i. Testing of magnetic computer tapes no more than six months ***prior*** to using them to store electronic records that are unscheduled or scheduled for permanent retention. This test should verify that the tape is free of permanent errors.

ii. Public entities should maintain the storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the temperature and relative humidity ranges set forth below:

Constant temperature -- 62º to 68º F

Constant relative humidity -- 35% to 45%

iii. Annually read a statistical sample of all reels of magnetic computer tape containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss.

iv. Copy permanent or unscheduled data, on magnetic tapes before the tapes are ten years old, onto tested and verified new tapes.

v. External labels for magnetic tapes used to store permanent or unscheduled electronic records should provide identification for each reel, including the name of the organizational unit responsible for the data, system title, and security classification, if applicable.

(3) Maintenance of direct access storage media:

(a) Issue written procedures for the care and handling of direct access storage media, which draw upon the recommendations of the manufacturers.

(b) External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records should include the following information:

i. Name of the organizational unit responsible for the records;

ii. Descriptive title of the contents; dates of creation;

iii. Security classification, if applicable;

iv. Identification of the software and hardware used.

(4) If the media contains permanent records and does not meet the requirements for transferring permanent records to State Archives, permit the migration of the permanent records at the time of transfer to a medium, which does meet the requirements.

Additional Consideration for Selection of Storage Mediums

The following factors should be considered before selecting a storage medium or converting from one medium to another:

(a) The authorized life of the records, as determined by the appropriate record series listed in the Statewide Records Retention Schedule;

(b) The maintenance necessary to retain the records;

(c) The cost of storing and retrieving the records;

(d) The records' density;

(e) The access time to retrieve stored records;

(f) The portability of the medium, i.e. selecting open standards media that will run on equipment offered by multiple manufacturers, and the ability to transfer the information from one medium to another, such as from optical disk to magnetic tape.

Section 9: Retention and Disposition of Electronic Records

The Records Conservation Board and the Supervisor of Records must approve disposition schedules. Records, including those in electronic format, may only be deleted or destroyed in accordance with the Statewide Records Retention Schedule and an approved application for destruction (Form RCB-2).

In order to achieve compliance with existing requirements, public entities need to establish policies and procedures to ensure that electronic records and their documentation are retained as long as required by the applicable retention schedule. These retention procedures should include the following provisions:

(1) Scheduled disposition of all electronic records, as well as related documentation and indexes, by applying the Statewide Records Retention Schedule.

(2) Scheduled Transferring of copies of permanent electronic records and any related documentation and indexes to the State Archives facility or other approved facility for the safekeeping of permanent records. Transfer may take place at an earlier date if convenient for both the public entity and the State Archives.

(3) Established procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle.

(4) Electronic mail records may not be deleted or otherwise disposed of without prior disposition authority from the Records Conservation Board, unless the electronic mail record is scheduled as "administrative use" and the administrative value for retaining the record has ceased. Electronic mail records scheduled as "administrative use" may be disposed of without further permission once the administrative use of the record has ended.

For more information on "administrative use" records, and retention requirements for correspondence, see the Statewide Records Retention Schedule.

(5) *Other records in an electronic mail system:* When a public entity has taken the necessary steps to retain a record in a scheduled recordkeeping system, whether electronic or paper, the identical version that remains on the user's screen or in the user's electronic mailbox has no continuing value.

(1) Deletion of the version of the record in the electronic mail system is permitted after the record has been preserved in a recordkeeping system along with all appropriate transmission data.

(2) The disposition of electronic mail records that have been transferred to an appropriate recordkeeping system is governed by the records disposition schedule, or schedules, that control the records in that system. If the records in the recordkeeping system are not scheduled, the public entity must follow the procedures outlined herein to schedule the record.

(6) No electronic record should be disposed of if it is subject to a public record request or likely to be subject to a dispute, audit, investigation, or litigation, or subject to other legal retention requirements, regardless of the public status of the record. Individuals should consult their agency attorney if there is any question as to whether a particular electronic mail message is relevant to an ongoing dispute, investigation or litigation.

Section 10: Destruction of Electronic Records

Records, including those in electronic format may only be deleted or destroyed in accordance with the approved disposition schedule and an approved application for destruction (Form RCB-2).

In order to achieve compliance with the existing requirements, public entities need to establish policies and procedures to ensure that electronic records and their documentation are destroyed only in accordance with applicable laws, as well as the records disposition schedule approved by the Records Conservation Board. At a minimum, each public entity should ensure that:

(1) Electronic records scheduled for destruction are disposed of in a manner, consistent with the provisions of G. L. c. 93I, that ensures protection of any sensitive, proprietary, public safety or security information.

(2) Magnetic recording media previously used for electronic records containing sensitive, proprietary, public safety or security information are not reused if the previously recorded information cannot be properly destroyed or rendered unreadable.

(3) Procedures are established and implemented that specifically address the destruction of electronic records generated by individuals employing any electronic mail system.

Section 11: Accessibility to Public Information for Persons with Disabilities

With some exceptions, Federal and State laws require that public sector agencies make public documents accessible to persons with disabilities.

In order to achieve compliance with the existing requirements, public entities need to address how public information will be made accessible to persons with disabilities.

Note: Executive Department agencies are required to comply with the Enterprise Information Technology Accessibility Standards and the Enterprise Web Accessibility Standards.

(1) Electronic records should be formatted in accordance with manufacturers' directions related to accessibility in a format that is verifiably accessible to persons with disabilities.

The following is a non-exhaustive list of formats that are accessible to persons with disabilities when applied correctly:

- .doc
- .pdf
- .html
- .xml
- .txt
- .asci

(2) In those rare cases where preservation of the appearance of the original document is of legal or historic significance and it is not possible to both make the document accessible and preserve its original appearance, accessibility shall be accomplished by creation and retention of a second accessible document.

Section 12: Conclusion

Any questions from agency records custodians regarding these Guidelines should be addressed to the Supervisor of Records, the Records Conservation Board, or the Information Technology Division.

Appendix A

Definitions for the Purpose of these Guidelines

Note: The Records Conservation Board may revise the definitions from time to time as used in these Guidelines to reflect applicable technological advancements.

Agency: A department, bureau, commission, board, office, council, or other entity in the executive department of government, which was created by the constitution or statutes of the Commonwealth of Massachusetts.

Data: Any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Database: An electronically stored set of data, consisting of at least one data file, which is sufficient for a given purpose.

Database management system means a software system used to access and retrieve data stored in a database.

Desktop documents means text, spreadsheet, presentation, calendar, task list, contact and other documents created through the use of software by individual users for their work-related purposes regardless of where it is stored.

Document: A document is a form of information. A document can be put into an electronic form and stored in a computer as one or more files. Often, a single document becomes a single file. As files or data, a document may be part of a database. When using certain computer application programs such as a word processor, a document is the unit of saved work. Each document is saved as a uniquely named file.

Duplicate electronic mail message, also referred to as duplicate email, means an electronic mail message that is a copy of another electronic mail message with the same message content including attachments.

Electronic means relating to technology as having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Electronic information system means a system that contains and provides access to computerized agency records and other information.

Electronic mail message, also referred to as email, means a document created or received on an electronic mail system including: brief notes, more formal or substantive narrative documents, and any attachments, such as word processing, spreadsheet, presentation and other electronic documents which may be transmitted with the message, as well as any information related to the transmission of the message.

Electronic mail system refers to the technology used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities, software that transmits files between users but does not retain any transmission data, data systems used to collect and process data that have been organized into data files or data bases on either personal

computers or mainframe computers, and desktop documents not transmitted on an electronic mail message system.

Electronic record means a record created, generated, sent, communicated, received or stored by electronic means.

Electronic recordkeeping system means an electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

Floppy Disk: A random access, removable magnetic data storage medium that can be used with personal computers. These types of disks are convenient for storing individual files and small programs.

Information Technology Division, also referred to as ITD, means the Information Technology Division, a division of the Executive Office for Administration and Finance established by G. L. c. 7, § 4A(d).

Long Term Storage refers to any retention that is needed for longer than 10 years.

Magnetic Media Storage Device: A magnetic storage device is a device that uses a magnetic head to read and write data to and from a "magnetizable" medium. The medium can be as basic as a plastic tape that is coated with fine particles of a metal, such as is found in audio recording and tape storage devices. Other examples include a floppy disk drive, a tape drive and a computer's hard drive.

Metadata means information describing the history, tracking, or management of an electronic document. Examples of metadata include: file designation, create and edit dates, comments, authorship, and edit history.

Portable storage media means any removable storage media. For the purpose of these Guidelines, portable storage media may include: flash drives, thumb drives, USB devices, CD's, DVD's, external hard drives, laptops, and smart phones.

Public entity means any entity subject to the provisions set by the Records Conservation Board pursuant to the authority granted in G. L. c. 30, § 42.

Receipt data means information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Records Conservation Board, also referred to as the RCB, means the Board, organized by G. L. c. 30, § 42, charged with setting the standards for the management of state records.

Records custodian: Custody of public records is in the office that creates, receives or maintains the records for use. Each officer in charge of a government office or department is the custodian of the records held by that office or department and has the primary responsibility for ensuring the safety of the records, providing access to those records and ensuring their authenticity. Any entity maintaining the records is acting as an agent of the record custodian, providing only for the physical care of the record, and may not take action with respect to the records without the specific authority of the custodian.

Social media: Websites that facilitate user participation, social interaction, collaboration and information sharing through the submission of user generated content. Some examples of social media tools include wikis, blogs, Facebook, and Twitter.

Supervisor of Records, also referred to as the Supervisor of Public Records, means the officer under the aegis of the Secretary of the Commonwealth statutorily designated pursuant to G. L. c. 66, § 1 to take necessary measures to put the records of the Commonwealth, counties, cities or towns in the custody and condition required by law and to secure their preservation.

Transmission data means information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.