Library of Virginia Electronic Records Guidelines

Electronic records have transformed the way Virginia's state agencies and localities create and share information. From databases to email to social media, electronic records have largely replaced their paper predecessors. While the landscape has changed, the requirement remains to properly manage records in accordance with public records law.

Virginia's state and local agencies are required to manage all public records, including electronic records, according to the Virginia Public Records Act, or VPRA (*Code of Virginia* § 42.1-76–§ 42.1-91). The VPRA outlines the recordkeeping responsibilities of government employees, defines the scope of public records, and describes requirements for securing, retaining, and disposing of public records. The VPRA defines public records as follows:

> *"Public record" or "record" means recorded information that documents a transaction or activity by or with any public officer, agency, or employee of an agency. Regardless of physical form or characteristic, the recorded information is a "public record" if it is produced, collected, received, or retained in pursuance of law or in connection with the transaction of public business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a "public record."*
>
> - *Code of Virginia* §42.1-77

The value of information is determined by *content*, not its *format.* The content determines the value and how long the information must be retained. The same applies to electronic records. The value and retention period are determined by the informational content of the electronic record, rather than the specific format (Word, spreadsheets, databases, etc.). An agency's electronic records can have various retention requirements depending on the information they contain.

These guidelines describe general principles for managing electronic records, as well as specific guidance for common types of electronic records. Furthermore, these guidelines identify critical issues for public officials to consider when designing, selecting, implementing, operating, and maintaining an electronic records system.

The guidance is applicable to all state agencies, local government entities and regional authorities within the commonwealth as defined by the Code of Virginia.

Electronic Records Guidelines (Full Text)

Chapter-by-Chapter:

Public records, including electronic records, document and provide evidence of public business conducted in Virginia. As such, it is essential that these records are trustworthy. Agencies should consider the characteristics of trustworthy records when development or selecting recordkeeping systems.

What are the essential characteristics of electronic records?

Before learning what makes a record trustworthy, let's first look at the three essential characteristics of records:

1. Content
   The content of a record is the information it conveys. Content can be composed of numbers, text, symbols, data, images, or sound. The content of a record should provide accurate information about a function or activity.

2. Context
   Contextual information is crucial to the evidentiary function of records. If a record lacks key information about its creator, the time of its creation, or its relationship to other records, its value as a record is severely diminished or lost entirely. In addition to serving an evidentiary function, contextual information also makes records easier to retrieve, use, and share. In the case of electronic records, contextual information is typically embedded into the record's metadata.

   Metadata is data describing the context, content, and structure of electronic records and their management through time. Effective metadata relies on a structured format and controlled vocabulary that is commonly understood among its creators and users.

3. Structure
   Structure is defined as the appearance and arrangement of a record's content, including the relationships between fields, entities, language, style, fonts, page and paragraph breaks, and links. Recordkeeping systems must capture and preserve information about the structure of records either as part of the metadata associated with the records or in separate documentation.

The characteristics of content, context, and structure can be evaluated to determine whether the record is trustworthy.

What are the characteristics of trustworthy electronic records?

There are four characteristics of record trustworthiness: reliability, authenticity, integrity, and usability. Electronic records should be stored in a system configured for records management that enables agencies to confidently store, manage, and retrieve records while maintaining these four characteristics:

1. Reliability

The system should be dependable and support processes of confidentiality, evidence, access, distribution, preservation, and destruction. It should be capable of preserving records in a consistent and accurate manner. It should employ a simple record structure based on open standards and non-proprietary file formats. This approach enhances reliability by avoiding dependence on a specific company or organization.

2. Authenticity
   The system should guarantee the authenticity of records, meaning that their context, content, and structure can be verified and trusted by metadata, audit trails, and other information that validates the integrity of the records.

   Metadata should always be collected, structured, and maintained with the record at the time of record creation. Most software applications automatically create metadata and associate it with files. One example of metadata creation is the header and routing information that automatically accompanies an email message. Another is the set of properties created with Microsoft Word documents – certain elements such as the title, author, and file size can be automatically created. Some systems allow you to customize metadata and/or create it manually to further support the record's authenticity.

   To increase the value of both metadata and the information it describes, work with creators, custodians, and users of information. By collaborating on metadata standards, tools, and practices, a more beneficial and compliant information management program is created.

3. Integrity
   The system should protect records against unauthorized alteration or deletion. It should employ security measures such as access controls, encryption, and audit trails to ensure the integrity of records and prevent unauthorized modifications.

   To maintain record integrity, agencies should follow the IT professions' best practices for data preservation. Systems should ensure the following:

   - A record creator's identity is verified
   - Restrictions exist regarding permissions to read and write files
   - Data transmission includes data error checking and correction
   - Data backup occurs regularly
   - Data on off-line storage media are regularly refreshed to avoid loss of data due to degradation
   - Periodic system audits are conducted and used to iteratively improve the records program

4. Usability
   The system should provide efficient and user-friendly functionalities for managing and accessing records. It should support search capabilities, retrieval, and other features that enable users to locate and utilize records effectively, provide records in compliance with open records laws, and manage and dispose of records in compliance with public records laws.

Many legacy and current records systems used by agencies do not have the capacity to ensure trustworthiness. However, it's important that agencies evaluate their systems according to the features of trustworthiness above and work towards solutions that can capture and maintain the essential

characteristics of electronic records for their full lifecycle. The trustworthiness of electronic records is only as credible as the governance put in place to manage the information lifecycle.

Most of the day-to-day records that Virginia's government agencies create – documents, presentations, images, or audio/visual materials – are unstructured records. Unstructured records can be defined as information that is *not* uniformly stored in a structured database format.

I. What are the challenges of managing unstructured records?

- Discoverability
  Because of their diverse and dispersed nature, unstructured records can be difficult to efficiently locate (discover) and manage.

- Security
  Unstructured records can be at risk from internal breaches (unauthorized staff accessing the records) as well as external breaches (cybersecurity threats).

- Over-Retention
  Unstructured records do not exist in a structured system that can automate retention and disposition. Unless agencies establish and adhere to a process for manually identifying retention periods and implementing disposition, unstructured records are prone to over-retention, which increases liability for the agency.

- Preservation
  As hardware and software become obsolete, or data is corrupted or degraded, unstructured records can become inaccessible.

Addressing these challenges requires organizations to implement effective records management strategies, including the adoption of trustworthy repositories, robust security measures, clear retention and disposition policies, and proactive preservation strategies. By doing so, organizations can enhance the discoverability, security, and long-term accessibility of their unstructured records, mitigating risks and maximizing the value of their information assets.

II. Where should unstructured records be stored?

Unstructured records are diverse and can appear in various formats and locations, such as external hard drives, shared network drives, or cloud servers. For optimal management and preservation, the ideal location for completed, approved, or inactive unstructured records is a trustworthy system or repository. For more information, see LVA's guidelines on Trustworthy Electronic Records.

It's worth noting that cost considerations currently limit the adoption of ECM systems or similar trustworthy digital repository solutions for most state agencies and localities. Given the current limitations, organizations can manage unstructured records manually by following these steps:

- Move completed, approved, or inactive unstructured records to a central shared location such as a network drive that is accessible to all relevant users. This will help ensure that users are working on the official and most updated versions of files, that those files are

properly designated, maintained, and managed as public records, and that records are not lost during employee turnover.

- As much as possible, incorporate access controls to ensure security. Establish procedures that indicate which users may access which records, and what permissions those users must have to edit records.
- Incorporate version controls to ensure accuracy and reduce the proliferation of multiple or outdated versions. Enforce read-only status on files to prevent unauthorized changes.
- Organize records based on their retention requirements, as mandated by the appropriate General Schedules for Localities, General Schedules for State Agencies, or Specific Schedules for State Agencies.
- Work with IT to ensure that unstructured records are properly backed up on a regular basis, to facilitate recovery. Follow the 3-2-1 strategy of data storage: at least three copies, stored on two different media, with at least one copy stored offsite.
- At the end of the records' lifecycle, follow the requirements for their disposal by completing the online RM-3 form, "Certificate of Records Destruction," and subsequently destroying the records.
- Explore the retention capabilities of your system, including options for adding retention tags or labels to records.

By implementing these manual management practices, organizations can still maintain some level of control over their unstructured records until more cost-effective and comprehensive solutions become more accessible in the future.

> ***The remainder of this guidance document will focus on managing unstructured records that are commonly stored on external hard drives, shared network drives, or cloud servers. These locations represent the most prevalent storage options for unstructured records.***

III. How should unstructured records be stored?

Typically, the software in which a file is created has a default or native format, indicated by a file name suffix (e.g., .pdf). Many software programs allow users to select from a variety of formats when saving a file.

When selecting a file format, consider the retention and disposition of the record series to which the file belongs. Records with a short-term retention (0-7 years) can be retained in their native format with minimal risk of obsolescence. On the other hand, records with a long-term (longer than 7 years) or permanent retention will likely need to be migrated from their native format to more stable, high-quality formats to prevent obsolescence.

For a list of acceptable and preferred formats for each given file type, see the National Archive and Records Administration's (NARA) Appendix A: Tables of File Formats. Files with a long-term or permanent retention should be maintained in a preferred format.

IV. How should unstructured records be named?

Agencies should create procedures that establish requirements for the naming and arrangement of records within a shared filing system. All users should follow these procedures to save files according to the established naming approach and in the appropriate location.

Folder and files names should be descriptive and identify the contents and context of the record. Keep the following considerations in mind when developing a naming policy:

- Consistency
  No matter the naming approach, consistency is the key to accessibility.

- Uniqueness
  Names should be unique regardless of their location.

- Universality
  Names should make sense to all users, not just the user who created the file. Limit abbreviations or codes that might cause confusion.

- Conciseness
  Keep names concise to contain only the information needed.

- Scalability
  Think about the number of files or file versions needed. If a particular group of records grows quickly, do not limit numerical placeholders to two spaces, or only 99 records may be created within the group.

- Special characters
  Avoid commonly prohibited characters such as / ? < > \ : * | " ^
  Spaces, underscores, or hyphens are acceptable.

- Depth and breadth
  Avoid a file structure that is too broad or too deep. Spread out records among high-level folders and sub-folders. If many high-level folders contain too many files, divide files into additional sub-folders. If too many sub-folders contain few files, consolidate files in fewer sub-folders. Limit the depth of the file structure to 3-4 levels.

Within most systems, folders and files can be sorted alphabetically by name. Folder and files names therefore provide the foundational arrangement for your unstructured records. Users can take advantage of this to create names that enhance retrievability.

If it makes most sense to order files alphabetically, then begin the file name with a description of the content followed by the date. Conversely, if it makes more sense to order files chronologically or numerically, begin the file name with the date or number followed by the description of the content.

V. What are the components of a name?

Names should be descriptive, concise, and consistent. The highest-level folders should correspond with core business functions. Sub-folders may create further distinctions based on subject, date, event, or other components.

In developing a file-naming procedure, include the following minimum components:

- Name of creator or group associated with the file
- Description of content (ideally including the record series title or number)
- Date created or last revised
    - The LVA recommends a Year-Month-Date format, e.g., 2020-07-01.

Including the created or last revised date in the file name ensures that the most recent version of the file is clear, and that the date stays intact even if the file is copied or moved elsewhere. Copying or moving a file may change the last modified date in the file's system-generated metadata.

If the files are in progress, superseded, or obsolete, consider adding these additional components:

- Status (Draft, Final, Obsolete, Superseded)
- Version number

Below is an example folder/file structure based on a few common record types: board meeting minutes, agendas, and packets (where the board is mandated by the Code of Virginia or the Virginia Administrative Code).

- BoardName-MeetingMinutes-100338
    - 2022-03-01-BoardName-Minutes-Final
    - 2022-06-01-BoardName-Minutes-Final
- BoardName-MeetingAgenda-100305
    - 2022-03-01-BoardName-Agenda-Final
    - 2022-03-01-BoardName-Packet-Final
    - 2022-06-01-BoardName-Agenda-Final
    - 2022-06-01-BoardName-Packet-Final

VI. What are the retention requirements for unstructured records?

Retention and disposition schedules, available on the Library of Virginia website, prescribe required retention periods and destruction methods for all public records. The schedules contain lists of record series, or groups of records that serve a common function. Unstructured records may fall into various record series depending on the function they serve.

VII. How should unstructured records be destroyed?

For instructions on destroying electronic records, see LVA's guidelines on Destroying Electronic Records.

VIII. How should unstructured records be preserved and/or transferred to the Library of Virginia?

For instructions on preserving and transferring electronic records to the Library of Virginia, see LVA's guidelines on Preserving and Transferring Electronic Records. [Forthcoming in 2024]

Structured records are commonly stored in relational databases and have associated metadata that correlates them to other records within the database. Within a database, you might find compilations of discrete data (for example, a name or number) or electronic objects (for example, a PDF). Whether the information is discrete or more complex, if it documents the transaction of public business, then it fits the definition of a "public record" according to the Virginia Public Records Act.

Common examples of structured records include but are not limited to: information stored in document management systems, customer relations management systems, asset management systems, and human resource management systems.

I. What are the challenges of managing structured records?

- Lack of Records Management Functionality
  Some structured records systems simply do not have records management functionality. Other systems may provide the functionality, but at additional cost.

- Classification
  If structured records are used for several purposes, it can be challenging to classify them according to a specific record series in a records retention and disposition schedule.

- Destruction
  If a system is not designed with retention and disposition in mind, it is possible that destroying data within the system can affect relationships within the database, thereby causing technical issues.

- Discovery
  Due to the high volume of data and records stored in structured systems, discovery can be time-consuming and costly.

- Maintenance and Migration
  When systems become obsolete or can no longer be maintained, the data and records still within retention must be migrated to preserve their integrity and accessibility. Migrating records can be time-consuming and expensive.

- Over-Retention

Because of the numerous challenges in applying retention and disposition to structured records, many agencies and users decide to keep everything indefinitely. This increases liability for the agency in many ways, including the ongoing costs of storage, migration, and staff time.

II. How should structured records be stored?

Structured records systems should be designed with records management in mind from the beginning. When building or selecting a system, agencies should ensure that the system has the ability to manage records by their appropriate records retention and disposition schedules. If contracting with external providers to build or host systems containing public records, the contract should likewise require the vendor to manage the public records in compliance with the schedules.

Below are a few questions to keep in mind when building or selecting a system:

(1) Which record series will be stored in the system? What are the retention requirements for that series?
(2) If there are multiple series, can the system classify those records according to their series?
(3) Can the system assign the appropriate retention period to a records series based on the scheduled retention requirements?
(4) If the record retention is based on a specific trigger or event (such as the end of a fiscal/calendar year, employee separation, the closure of a case, or an audit) can the system apply retention periods based on those events?
(5) Can the system search and retrieve records for the purposes of FOIA, discovery, and access?
(6) Can the system securely migrate records to other systems?
(7) Can the system achieve the final destruction of records in a way that they are non-recoverable?
(8) If the records contained in the system have a Permanent/Archival disposition, can the system export records in a format suitable for transfer to an in-house electronic archives or to the Library of Virginia?

Unlike unstructured records, structured records have associated metadata that gives them context and correlates them to other records. Metadata is data that describes or gives information about other data – in other words, "data about data." Rich metadata facilitates the efficient discovery, management, and organization of data within a system, and is one of the primary advantages of structured records.

Descriptive metadata describes the record, and thereby facilitates discovery and retrieval. Structured records should ideally include the following descriptive metadata:

- Record Series Title and Number
- Unique Identifier

- Creator
- Date/Time
- Location

Administrative metadata provides information to facilitate the management of the record, and should ideally include the following:

- Retention Period
- Sensitivity Level (to aid in responding to records requests under the Virginia Freedom of Information Act)

While there are other types of metadata, descriptive and administrative metadata are essential for records management and can even enable automation of records discovery, retention, and disposition.

III. What is the retention period for structured records?

Retention and disposition schedules, available on the Library of Virginia website, prescribe required retention periods and destruction methods for all public records. The schedules contain lists of record series, or groups of records that serve a common function. Structured records may fall into various record series depending on the function they serve.

While structured records *can* be stored indefinitely, it is crucial to adhere to the retention requirements outlined in LVA's records retention and disposition schedules. Over-retaining structured records is a violation of the Virginia Public Records Act and creates liability for the agency.

IV. How should nonpermanent structured records be destroyed?

For instructions on destroying electronic records, see LVA's guidelines on Destroying Electronic Records.

V. How should structured records be preserved and/or transferred to the Library of Virginia?

For instructions on preserving and transferring electronic records to the Library of Virginia, see LVA's guidelines on Preserving and Transferring Electronic Records. [Document forthcoming in 2024]

Managing Email

Email is an essential tool for communication, collaboration, and the efficient delivery of public services and programs. From a records management perspective, email also provides documentation of government business and must be managed in a way that facilitates records retention, accessibility, and the preservation of knowledge.

I. What is the scope of email?

Email is a communication sent or received via electronic mail applications. It can include textual, numeric, graphic, or other information. The scope of email includes the metadata associated with the email record. Examples of common email metadata include but are not limited to:

- Names/email addresses of the sender and recipient(s)
- Time/date
- Subject line

An email record may contain attached files. The attachment may be considered an essential component of the email record if it is unique and is not readily accessible elsewhere in the agency's official recordkeeping system.

II. What are the challenges of managing email?

Like the management of unstructured records, the primary challenge in managing email records arises from the lack of records management tools specifically designed for email. If an automated tool is not available, email must be managed manually throughout its entire lifecycle.

Other challenges of managing email include:

- Volume
  A significant challenge of email is the volume that is created daily. Without a process for managing the volume, email quickly piles up and becomes unmanageable.

- Discoverability/Retrievability
  Because email accounts are managed by many individual users, rather than a shared group, email messages are often organized in non-uniform ways. This can make discoverability and retrievability of email records challenging. Most people rely on the email application's search bar, which offers limited search capabilities.

- Preservation
  Email can be prone to loss or inaccessibility when employees leave their positions. Without taking intentional steps to preserve the email of departing employees for the required retention period, an agency may become out of compliance with the Virginia Public Records Act.

III. What is the retention requirement for email?

There is no single retention requirement for email. Just like an envelope sent through the mail, email can contain a variety of information. Email is the format or the container for the record, not the record

itself. The content of an email, if determined to be a record, must be retained according to the records retention and disposition schedules available on the Library of Virginia website. The schedules prescribe required retention periods and destruction methods for all public records. They contain lists of record series, or groups of records that serve a common function.

Most email falls into the category of correspondence. There are several record series that deal with correspondence in the general schedules for Administrative Records (GS-101 for state agencies and GS-19 for localities). The retention for these series can range from zero years to permanent, depending on the creator and the content of the email.

Correspondence may also fall into other record series throughout the general and specific schedules. For example:

- Correspondence related to the administration of a funded grant program may fall into Grant Records: Funded (GS-101-100323 or state agencies or GS-19-010051 for localities)
- Correspondence with vendors may fall into Vendor Files (GS-102-012154 for state agencies or GS-02-200391 for localities)
- Correspondence containing requests for employee tuition assistance may fall into Education Assistance Program Records (GS-103-100481 for state agencies or GS-03-010229 for localities)
- Correspondence related to the proposal of legislation may fall into Legislative Case Files (GS-101-007136 for state agencies; N/A for localities)

On the other hand, email may be considered a non-record if it is duplicative or does not document official business. Common examples of non-record emails include:

- Emails received for reference, for which the recipient is not the responsible party within the agency
- Personal emails
- Emails with attachments, when the attachments are stored elsewhere on the agency's official recordkeeping system
- Meeting information that is duplicated in the calendar event (e.g., accepted/declined notifications)
- Listserv/distributed emails
- Spam/promotional emails

IV. Where should email be stored?

Agencies and localities typically have limited or no choice about which email application is used. Ideally, however, the email application should meet the following criteria:

1. Email is discoverable and retrievable
2. Email can be retained for its designated retention period and then destroyed
3. IT can place a hold on emails as needed for FOIA, discovery, audit, etc.
4. The trustworthiness of the email can be preserved

For more information about trustworthiness, see LVA's guidelines on Trustworthy Electronic Records.

V. How should email be governed?

Email applications are gradually strengthening in their records management and compliance functionality, which has made it more feasible to apply classification, discovery, retention, and disposition within the system configurations. Examples of this functionality include:

- Retention policies – assigns a retention period to a user's mailbox
- Retention labels – assigns a retention period to an item (e.g., a specific email or folder)
- Sensitivity policies – assigns a security classification level to a user's mailbox
- Sensitivity labels – assigns a security classification to an item (e.g., a specific email or folder)
- Holds (legal, FOIA, audit, etc.)

If these automated tools are not available, see "How should email be organized?" below for tips on manual organization, retention, and disposition.

Whether automated or manual, email management practices should be formalized and enforced through the agency's internal policies. Policies should establish procedures for email storage, classification, security, retention, and disposition. Agency employees should receive training on the agency's email management practices.

VI. How should email be organized?

If the email application is capable of automating email retention, the LVA recommends creating retention policies and labels based on the records retention and disposition schedules. If organizing email manually, the LVA recommends using folder structures, categories, or other available metadata to sort and label email in a way that facilitates discovery, retention, and timely disposition.

VII. How can confidential email be protected?

Public records, including email, are not necessarily open to the public under the Virginia Freedom of Information Act (FOIA). The Code of Virginia allows disclosure exemptions for certain public records. Nevertheless, the rules for records retention and disposition stay the same.

Agencies should implement tools or systems that identify the sensitivity level of email messages. Only emails that contain sensitive information should be labeled as such. Agencies should *not* apply blanket policies that identify all email as sensitive.

VIII. What should be done about a departing employee's email?

Agencies should take steps to ensure that the email of departing employees is retained for its applicable retention period.

If an employee's mailbox contains non-permanent emails, the agency can either:

1. Apply retention rules within the user's live mailbox
2. Export the user's email to an offline storage format and retain it for the longest identified retention period

If an employee's mailbox contains permanent emails, the agency should promptly follow procedures for transferring those records to the agency's archives or the Library of Virginia, per the stated series disposition.

IX. How should email be destroyed?

For instructions on destroying electronic records, see LVA's guidelines on Destroying Electronic Records.

X. How should emails be preserved and/or transferred to the Library of Virginia?

For instructions on preserving and transferring electronic records to the Library of Virginia, see LVA's guidelines on Preserving and Transferring Electronic Records. [Document forthcoming in 2024]

Managing Web and Social Media Records

Virginia's state agencies and localities rely on websites and social media to engage with the public and provide information about agency services. Before these online tools existed, agencies shared information through paper newsletters, announcements, and other publications. While the format has evolved, any records created on agency websites and social media must still be managed in compliance with the Virginia Public Records Act.

Currently, most agencies and localities use websites and social media sites to:

- Publicize information
  Promote agency services. Announce upcoming events, job openings, and changes to policies or procedures. Notify the public of changes to services and events and provide real-time updates.

- Facilitate outreach
  Receive comments, answer questions, and participate in two-way communication with constituents.

This document provides guidance on managing web and social media records, including how to identify what does and does not constitute a public record, determine retention and disposition requirements, create policies governing web and social media, and preserve web and social media records for future generations.

I. What are the challenges of managing web and social media records?

- Education
  Communications or senior management staff are usually responsible for managing agency or locality websites and social media. Records management may not be their primary focus, so they may need additional education to understand public records law, what constitutes a record when it comes to the web, and how to manage, store, and preserve these records.

- Moderation
  Moderation refers to the management and monitoring of online content to ensure that it complies with agency or locality policies and legal requirements. Both internal and external moderation should be considered when creating a website/social media policy.

- Internal moderation includes defining which agency staff are authorized to manage the website/social media, who is responsible for what, security protocols, and requirements for preserving the online content.
- External moderation includes defining rules for public users, types of banned content or behavior, and how to moderate this content while still preserving it as a record.

- Ownership and Accessibility
  Most social media sites are owned and operated by a third party (e.g., Facebook, Instagram, YouTube, or TikTok). Under the terms of service, the social media site can remove content as it sees fit. The agency does not have ownership of posted content. Additionally, if public comments are enabled, the agency does not have ownership or control of those comments. If users make and then delete comments, the agency cannot restore access to them. Before using any social media site, agencies should review the terms of service and make a plan for records management.

- Preservation
  Websites are updated frequently, so capturing and preserving information before it disappears is crucial. It's important to consider how often websites should be captured, and the scope of what should be captured. Social media presents the same challenges, but with the added complication that the agency does not own or control the platform. Platform obsolescence is a significant risk, as demonstrated by the rise and fall of sites like MySpace and Vine.

II. Is content posted on the web and social media a public record?

If your agency or locality uses websites or social media platforms, you need to know that online content may be a public record if it relates to the transaction of the agency or locality's public business. Public records in the commonwealth are subject to the Virginia Public Records Act, or VPRA (*Code of Virginia* § 42.1-76–§ 42.1-91).

1. What Constitutes a Public Record?

According to the VPRA, any information that documents the transaction of an agency's public business is considered a public record. This includes online content, since the VPRA specifies "regardless of physical form or characteristic" (§ 42.1-77). Examples of public records on websites might include text and images embedded in the webpage that do not exist elsewhere. Examples on social media might include posts that contain unique information not stored elsewhere; agency comments; or comments made by members of the public.

2. *What Constitutes a Non-Record?*

If the online content provides unique information that does not exist elsewhere, it is a public record that must be preserved and retained. On the other hand, if the online content duplicates information that an agency maintains elsewhere, then the content may be considered a copy and treated as a non-record. For example, an agency might post documents to a website or social media that also exist on the agency's network drive. If the content duplicates records maintained elsewhere, then the content is a non-record. Formatting existing content for posting, such as adding background colors, an agency logo, or other cosmetic changes, does not create a new record.

III. What is the retention requirement for web and social media records?

Records retention and disposition schedules, available on the Library of Virginia website, prescribe required retention periods and destruction methods for all public records. The schedules contain lists of record series, or groups of records that serve a common function. However, as with email, "the web" and "social media" are not records in and of themselves. Whether their content is a record depends on the function that they serve, with retention requirements ranging from zero years to decades, or even permanent archival preservation.

IV. How should web and social media records be preserved?

1. Verify if LVA is Archiving Your Website(s) and/or Social Media Site(s)

The LVA has partnered with Archive-It, a web-crawler and web-archiving service, since 2005 to crawl a select number of state agency websites. Agencies can check to see if their website/social media is already being captured by LVA by checking this link:

https://archive-it.org/collections/335

The primary purpose of Archive-It is to capture the look and feel of a site for historical purposes, *not* to serve as a compliance tool for the purposes of FOIA or e-discovery. Archive-It is limited in the frequency and depth of its crawls and may not capture files such as images, audiovisual content, or documents posted on a site. Agencies should ensure that files posted on a site are preserved by either using a vendor with more robust capture tools, or storing all posted files within the agency's recordkeeping system.

Note: If the URL of your agency website's homepage changes, please contact LVA so that Archive-It may be updated.

2. *Use a Vendor*

If LVA is not capturing an agency's site(s) via Archive-It, or if the agency requires a more robust capture tool for compliance purposes, then the agency can use a service provider to capture their websites and social media sites.

When considering providers, agencies should consider several factors:

- Size of the organization and volume of records
  Smaller agencies and localities, and those with smaller amounts of content may be able to capture their content using a simpler tool or process; while larger agencies and localities, or those with a high volume of content may require a more robust solution.

- Length of time needed to retain records
  The retention period may vary depending on the type of content. It's important to ensure that the tool selected can meet the agency's retention requirements.

- Frequency of Freedom of Information Act (FOIA) requests
  The Virginia FOIA gives citizens of the Commonwealth the right to access government information, with certain exceptions for protected information. If an agency or locality receives a high volume of requests, they may need a tool that can easily and quickly search and retrieve specific records and provide associated metadata to prove authenticity.

3. *Capture Sites on Your Own*

If LVA is not capturing an agency's website/social media, agencies can capture the sites on their own by either using a free online archiving tool such as the Wayback Machine.

Alternatively, agencies can capture sites by printing or screen-capturing the relevant web and social media records. Since this approach does not reliably capture metadata, however, it is not sufficient to comply with FOIA requests, legal discovery, or audits.

V. How should web and social media records be governed?

To ensure the preservation and accessibility of public records, agencies that maintain websites or social media should implement policies for the governance of these platforms. This can include developing a system for identifying public records, setting retention periods, and specifying the format and location

of the records. By implementing clear policies and procedures, agencies can ensure that they are complying with the VPRA and managing their online content in a responsible and effective way.

State agencies need to ensure that the policy also includes web accessibility standards, as required by the Department of Human Resource Management (DHRM) Policy 1.75:

> *"An agency using social media should be prepared to meet accessibility standards. Section 508 of the Rehabilitation Act (29 U.S.C. § 794d) requires that federal agencies' electronic and information technology is accessible to people with disabilities, and the commonwealth accepts the Americans with Disabilities Act as its legal standard, pursuant to Code of Virginia, § 2.2-2012… An agency using social media should be prepared to respond to Freedom of Information Act (FOIA) requests and should have considered how records retention and disposition requirements under the Public Records Act and applicable schedules apply to the agency's social media records." – DHRM Policy 1.75, page 6*

Local and regional government entities need to ensure they are in compliance with any similar policies.

VI. How should web and social media records be destroyed?

For instructions on destroying electronic records, see LVA's guidelines on Destroying Electronic Records.

VII. How should web and social media records be preserved and/or transferred to the Library of Virginia?

For instructions on preserving and transferring electronic records to the Library of Virginia, see LVA's guidelines on Preserving and Transferring Electronic Records. [Document forthcoming in 2024]

Managing Text & Instant Messages

Text messaging can be a convenient communication tool in professional settings. Some agencies issue government phones to employees, who then use text messaging for official business purposes. Likewise, instant messaging is increasingly used as an alternative to email via platforms such as Microsoft Teams.

Like other types of communication such as email, text messages and instant messages can be subject to records retention and disposition requirements outlined by the Virginia Public Records Act (VPRA).

I. What are the challenges of maintaining text and instant messages?

- Governance
  Agencies may find it challenging to apply records management processes to text and instant messaging, as the service providers often offer limited or no records retention or disposition functionality.

- Discoverability/Retrievability
  It can be difficult to search for and retrieve content from text messages using the device itself; however, it is possible to export the text messages to another device for easier review. Instant message platforms have better native search tools and capacity for organization using channels, but discovery and retrieval are still challenges given the volume of messages.

- Ownership and Accessibility
  Conducting government business via text message on a *personal* device, while convenient, should not be an agency-sanctioned method of communication. This is because text messages on a personal device are owned by the commercial service provider, rather than the agency, and cannot be accessed if the employee separates. Nevertheless, if used to conduct government business, text messages on a personal device may be subject to the retention and disposition requirements of the VPRA.

II. What is the retention requirement for text/instant messages?

There is no single retention requirement for text or instant messages. The content of the message, if it is determined to be a record, must be retained according to the LVA records retention and disposition schedules. The schedules contain lists of record series, or groups of records that serve a common function.

Most text and instant messages fall into the category of correspondence. There are several record series that deal exclusively with correspondence in the general schedules for Administrative Records (GS-101 for state agencies and GS-19 for localities). The retention for these series can range from zero years to permanent, depending on the creator and the content of the message.

Text and instant messages, like email, may be considered non-records if they are duplicative or do not document official business.

III. How should text/instant messages be governed?

Agencies should carefully consider whether to permit the use of text and instant messaging for conducting government business. ***The Library of Virginia strongly discourages all government employees from conducting government business by text messaging via a personal device.*** If permitted, then agencies should implement policies that govern the use of text and instant messaging. Users should receive training on policies, once implemented.

When developing an agency policy, consider how the agency will ensure the discovery, retrievability, retention, destruction, and preservation of text and instant messages. Within instant messaging platforms, explore whether the platform's settings include configurable retention policies. Keep in mind the Virginia Public Records Act's requirement to submit a Certificate of Records Destruction (RM-3 form) to the Library of Virginia before destroying public records.

IV. How should text/instant messages be destroyed?

For instructions on destroying electronic records, see LVA's guidelines on Destroying Electronic Records.

V. How should instant messages be preserved and/or transferred to the Library of Virginia?

For instructions on preserving and transferring electronic records to the Library of Virginia, see LVA's guidelines on Preserving and Transferring Electronic Records. [Document forthcoming in 2024]

Destroying Electronic Records

The records retention and disposition schedules provide authority for agencies to destroy public records once they have fulfilled their prescribed retention period. Records should be disposed of in a timely manner once the retention expires. The destruction of all public records must be documented and reported to the Library of Virginia through the submission of a Certificate of Records Destruction (RM-3 Form), as required by the Virginia Public Records Act (Code of Virginia § 42.1-86.1).

I. When can electronic records be destroyed?

The retention period of records, electronic or otherwise, depends on the content of the record rather than the format. Electronic records may fall into various record series with various retention requirements, depending on the information they contain. There is no single retention requirement for electronic records.

To determine the retention period, consult the records retention and disposition schedules: https://www.lva.virginia.gov/agencies/records/retention.asp

Consider whether the electronic records may be non-records as defined by the Virginia Public Records Act (Code of Virginia § 42.1-77). If the electronic records are duplicative or do not pertain to public business, they may be non-records. Non-records may be destroyed at any time, and the destruction should not be reported to LVA.

II. When can backups or duplicates of electronic records be destroyed?

It is advisable and common practice to create regular backups of electronic records, whether stored on-premise or in the cloud, that can be recovered if the original records are lost. Backups of electronic records created for recovery purposes are duplicative of the official records and therefore may be considered duplicative non-records.

Other duplicates of official records can also be considered non-records. For example, attached files sent via email might be duplicative if the official version is stored elsewhere on the agency's recordkeeping system. The proliferation of duplicates can create risk and liability for an agency. Avoid the proliferation of duplicates by sharing access to the official records and working collaboratively on them, rather than sharing and working on multiple versions.

As non-records, backups and duplicates may be destroyed at any time, and the destruction should not be reported to LVA via the Certificate of Records Destruction (RM-3 form). However, backups and duplicates of official records should be destroyed before or at the same time as the official records are destroyed; otherwise, the duplicates may be subject to discovery. If backups are maintained by a vendor, coordinate with the vendor to ensure backups are destroyed.

III. Where can I find the Certificate of Records Destruction (RM-3 Form)?

The Certificate of Records Destruction (RM-3 form) is an online form available on the Records Management Forms page on the LVA website: https://www.lva.virginia.gov/agencies/records/forms.asp

Underneath the RM-3 form, you will also find links to the following resources:

- RM-3 Preparation Instructions (pdf) (videos)
  - The PDF instructions provide detailed information on each step of the RM-3 form process.
  - The videos provide walkthroughs for each step of the RM-3 form process.
- Reporting Destruction Tip Sheet (pdf)
  - The tip sheet provides a few essential facts about destruction requirements and the RM-3 form.
- Volume Equivalency Table (pdf)
  - The table provides the volume (in cubic feet) of common records storage containers.
- In-Progress Dashboard
  - The dashboard allows anyone to monitor the status of a submitted RM-3 form. It shows where the form is in the approval process and the date it was last active.
- Completed Form Search
  - The search tool, available on the LVA website, allows anyone to search for and review the details of completed RM-3 forms. Users can search for RM-3 forms using many criteria, including specific agency information or specific information about the records.

IV. Why should electronic records be routinely destroyed?

The Library of Virginia recommends evaluating electronic records on a regular basis as part of an agency's routine file-cleanup process. Frequency of destruction (monthly, annually, etc.) may vary depending on the agency; the most important thing is that destruction occurs on a regular and consistent basis in order to minimize backlogs and establish a pattern of defensible disposition.

During the file cleanup, destroy electronic records that have fulfilled their retention requirements according to the retention schedules. At the same time, agencies should evaluate whether active web and social media records need to be migrated to another format to prevent obsolescence.

V. How do I determine the volume of electronic records being destroyed?

The volume of electronic records being destroyed must be reported in bytes (e.g., kilobytes, megabytes, gigabytes, terabytes, etc.). The volume should be as accurate as possible but may be an estimate. For many electronic records, the volume can be viewed within the file properties. If you are unable to determine the volume, consult IT staff or a vendor (if applicable) for assistance.

Byte conversions:
1 kilobyte (KB) = 1000 bytes
1 megabyte (MB) = 1000 kilobytes (KB)
1 gigabyte (GB) = 1000 megabytes (MB)
1 terabytes (TB) = 1000 gigabytes (GB)

VI. How do I destroy electronic records?

LVA recommends consulting IT staff or a vendor (if applicable) for assistance in destroying confidential electronic records.

Electronic records are either destroyed confidentially or non-confidentially, depending on the sensitivity of the content. To determine which method is required, consult the "disposition method" column of the retention and disposition schedules.

If the disposition method is Confidential Destruction, or the records are known to contain sensitive content, then they should be destroyed in a way that the information is not recoverable. Merely deleting confidential files is not sufficient, as the files can still be recovered following deletion.

Common confidential destruction methods include:

- Overwriting
- Electronic shredding or incineration
- Degaussing (for magnetic media)
- Physical destruction of storage device

If the disposition method is Non-Confidential Destruction and the records do not contain sensitive information, then the records may be simply deleted (by hitting the Delete key), or the storage device may be sent to a landfill or recycling center.

VII. How do I destroy electronic records when the current database system doesn't allow for destruction?

If an agency's existing system is not capable of destroying records, consider the following options:

(1) Retrofit the system to make disposition possible
(2) Migrate all records to a new system that meets requirements
(3) If the current system does not allow for migration, wait until all the records in the system have fulfilled their retention requirements, then dispose of all records within the system

VIII. How do I report the destruction of records that are destroyed automatically?

Some agencies have implemented systems that automatically purge records, e.g., audiovisual recordings, after a pre-determined period of time and, typically, on a daily basis. If the recordings document government business, then they are likely public records and are subject to retention and destruction-reporting requirements. Although not in strict compliance with the Public Records Act, reporting the destruction of already-purged records increases the defensibility of the destruction.

Some systems provide logs or reports of automated destruction which can be used to report destruction to LVA. Other systems do not provide logs, and therefore destruction is challenging to accurately report. For systems that do not provide logs, the LVA recommends following the below steps to estimate the file size of the records subject to destruction:

(1) Select a window of time for which destruction will be reported (monthly, quarterly, etc.)
(2) With the help of internal IT or the system's supplier/integrator, determine the estimated file size (in bytes) for a data set that spans the same length of the reporting window.
(3) Following the end of the window, report the destruction using the RM-3.

For ongoing destruction reporting of the same records series, the same steps can be taken to estimate file size, or the same estimate can be reported at regular intervals until there is reason to believe the volume has changed (e.g., additional recording equipment has been implemented).