ARCHIVES & HISTORY
General Commission on Archives and History
THE UNITED METHODIST CHURCH

Records Management Guidelines

Guidelines for Managing Digital Records

2024 Edition

The United Methodist Church General Commission on Archives and History
www.gcah.org

Guidelines for Managing Electronic Records
2017-2020

The United Methodist Church
P. O. Box 127
Madison, NJ 07940
http://www.gcah.org
gcah@gcah.org

2017-2020 Edition

PURPOSE

This publication provides guidance to general agencies and annual conferences on creating, managing and preserving digital records. Digital records must be actively managed in order to ensure they are available and usable for as long as required to support accountability, good ministry and the expectations of the public. All requirements relating to permanent and temporary records described in the Guidelines for Managing Records apply to electronic records as well (see 2016 Discipline ¶ 1711.1b). This document deals with issues unique to handling and preserving electronic records.

The guidelines contain advice on:
· the importance of managing digital records and how to manage them in an integrated way.
· best-practices to digitize commonly used records
· archivally preserving digital records for as long as they are required, including an overview of the General Commission on Archives and History approach.

Scope

The advice contained in these guidelines applies to all digital records created by agencies as evidence of their ministry activity. Digital records include all records that are created in a digital format (born digital), or have since been converted into a digital format. This document focuses on ways to manage and create digital files by staff, ways to transfer files to the archives, ways to digitize physical documents and methods for conferences and local churches to preserve their digital records.

These guidelines draw upon record keeping requirements for the management of digital records that are set out in GCAH's Guidelines for Managing Records and best practice standards. No document like this is written in a vacuum. It relies heavily on a variety of documents and studies from around the U. S. and around the world, including reports done by the U. S. National Archives, various states and the National Archives of Australia.

Audience

These guidelines should be used by all General agencies, episcopal offices and conference offices as a foundation to ensure that their digital records are managed appropriately. They are relevant to all agency staff and to those who digitize records as well as to conference archivists and local church historians.

Please note that for the purpose of this document electronic records and digital records are considered as synonyms.

Most of what is included in these guidelines are suggestions or "first steps" which can be taken by staff almost immediately to begin managing their records. By allowing and encouraging staff to take these first steps an agency can begin to incorporate into daily practice the necessary steps which will lead to a productive digital records management policy. The point being that such a policy should be introduced incrementally instead of all at once.

2017-2020 Edition

INTRODUCTION

Digital records must be managed for the same reasons records in other formats need to be managed. Records allow our ministry to be conducted efficiently and effectively. There are accountability and Disciplinary obligations that agencies must meet, and community expectations concerning the documentation and transparency of our actions. Further, special challenges, such as technological obsolescence and media degradation, make it imperative for digital records to be carefully managed.

Inadequate records and poor record keeping practices can contribute to accountability failures and inefficient performance. Effective record keeping strategies can lead to many benefits.

Records preserve an agency's history and form its corporate memory. Information about previous decisions and actions can improve service quality and effectiveness. Timely access to relevant data allows action officers to make decisions and do better ministry.

Managing digital records involves the following unique challenges:

· Digital technology evolves at a rapid rate. The software and hardware used by an agency to create digital records tends to be short-lived, quickly replaced by upgrades or improvements. Because of this hardware and software obsolescence, digital records can quickly reach a point where they cannot be read or understood. Yet, in order to meet agency obligations, records must remain accessible for as long as they are required.

· The general manipulability of digital records means that they can quickly and easily be updated, deleted or altered. However, digital records are evidence of ministry activity and must be managed to prevent unauthorized modification.

MANAGING FILES IN THE OFFICE

File Folder Structure

The first step is to organize your file structure on your PC and on your network folders. A well organized folder system will help you to keep track of your files. It will allow you to know what is current and what is completed.

The folder structure should follow your office filing system - if you have one - or it should reflect your work patterns and responsibilities. For example:

· There should be a folder for correspondence. And depending on the type of correspondence there may be a need for several sub-folders underneath the correspondence folder.

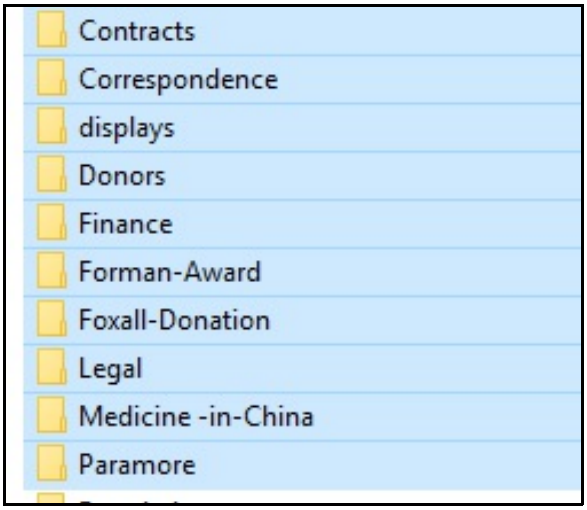

Figure 2 Sample File Folder Structure

· There should be a folder for reports and another for meetings. Again, there may well be the need for sub-folders for specific type of reports and specific meetings.

· Folders of completed projects or in some other way no longer being used should have the term "completed" appended to the folder. The way to edit or rename a folder depends on your operating system; highlight the folder name and in Windows press the F2 key to change the name; on a Mac press the Enter key to change/edit the name.

The file structure you create on your PC or network drives should also be mirrored in your e-mail. The two should be as similar as possible. Your e-mail will have additional folders related to work done exclusively with e-mail. Don't forget to edit folder names for completed projects here too.

If a folder has subfolders don't mix files with the subfolders.

Spending the time to create a coherent file structure will save you time in the long run and anyone else that needs to look at your files. If several of you work in one office or division it will help for everyone to have essentially the same structure - this will make job training easier. It is possible that your office has a standardized structure, or document management system, which manages this for you. If not it may be worth discussing in your office about setting us such a standard approach.

Naming Files

The task of giving every file a name is one of the great challenges of the digital era. In the past a report was just a report and went into a folder labeled reports. Now every document we create needs a name. Creating a useful name can be a real challenge.

· Create a name that is useful for you and your office. Make the name long enough that it will convey the content or purpose of the content.
· Avoid using too much short hand or code in creating a file name. Another staff person may need to find the document when you are not around. Be sure to help them with reasonable names.

· In order to make sure that your filenames last over time use 'dashes' in place of spaces when creating a file name: e.g. "Report of the Agency for 2016" to "Report-of-the-Agency-for-2016." Some operating systems will not accept filenames with spaces and using 'dashes' will ensure that your filenames are useable no matter what operating system is used in the future.

· You are naming files for the future. It could be for next week or 100 years for now, so make sure they are descriptive.

· Don't worry about your naming structure when your files go to the archives. The archival software will protect your file names and file structure.

File Control

Digital records are easy to share resulting in many copies of the 'same' file in several places around a computer or around a network. The best practice is to create one file and put it in a place where others can access it or to develop a linked file (known as a symlink) which allows users to have access to a

shared file but allows them to store the file in a convenient spot e.g. you could create a link to files on the network drive and have them appear in the appropriate folder on your hard drive. This reduces the number of actual copies on the system.

If multiple copies are on the system or shared with others via e-mail, your office needs to determine where the official copy is. This is important because electronic files are easily edited and an inappropriate edit could be mis-understood. You need a file which is the standard and to which all others can be compared.

This speaks to another element of your folder and file naming conventions. If you create an official document then you will need to mark that somehow as the official copy. It could be by placing it in a special sub-folder, or by changing the name to distinguish it from copies. This file should never be shared with anyone. Make a copy of the file and share that copy as well; edit the name so that it is recognizable as a copy or the original file. Store it on a folder with limited access. Do **not** protect it by placing a password on it; that is the same as deleting the file. Passwords should be avoided at all costs. Secure a file by placing it on a folder which has limited access.

When it is time to send these files to the Archives it is the official copies that you will send.

How Long Do Digital Records Need to Be Retained?

As with other formats of records, digital records need to be retained until they are no longer required for any purpose. There are three general reasons digital records need to be created and kept:

· to meet the requirements of legislation and accountability
· to support the efficient conduct of ministry
· to meet the expectations of the community.

Generally, digital records, as with other records, will fall into one of the following categories.

· Temporary value – the records can be disposed of at an identified time (e.g., "Destroy 7 years after action completed"). Temporary-value records can range in retention length from a very short period, such as one year, up to an extended period, such as "Destroy 13 years after date of birth (of subject)".

· Retain for a period of time in agency – the records have a long-term ministry use in the agency, but are not considered to have archival value.

· Archival value – the records cannot be disposed but instead will be retained in the custody of the Archives indefinitely. Agencies nominate groups of records when they develop a records disposal authority. GCAH decides which records meet the criteria for archival value.

A digital record must be managed, and remain accessible, for its lifetime. How long a digital record needs to be kept will influence its management. In these guidelines, we refer to "retaining digital records for the long term". Given the vulnerable nature of most digital media and the frequency of technology change, "long term" for digital records generally means longer than one generation of technology. Digital records that must be retained for the long term will require active management to ensure their continued accessibility.

Disposal of Digital Records

GCAH has produced guidelines for records retention which contain recommended disposal schedules for the episcopal offices and general agencies. A general agency is to produce its own retention guidelines, but they must be approved by GCAH before they can be placed into practice.

Normal Administrative Practice

Normal administrative practice (NAP) defines types of records that agencies may routinely destroy in the normal course of business. Agencies do not need to contact the Archives for permission to dispose of records within the scope of NAP. NAP usually applies to information that is duplicated, unimportant or only of short term facilitative value. For example:

· superseded system backups;
· trivial electronic messages that are not related to agency business;
· address lists and change of address notices;
· calendars, office diaries and appointment books (unless identified in a records disposal authority as having additional value);
· rough drafts of reports, correspondence, routine or rough calculations;
· routine statistical and progress reports compiled and duplicated in other reports;
· abstracts or copies of formal financial records maintained for convenient reference;
· duplicated material such as forms or templates;
· thermal paper facsimiles after making and filing a photocopy or scan.

The NAP provision must **not** be used to:
· destroy records of significant agency operations;
· destroy records that document the rights and obligations of the church or private individuals;
· cull documents within files; or
· destroy ministry-related electronic messages before they become part of the formal record.

NAP should **not** be applied to records or information that can be used as evidence.

When digital records are transferred to the Archives they will be deleted from the agency's server or network. Only the official record will be transferred to the Archives and then Archives will be the source of the official record; all others are copies which can be compared to the original when necessary.

Storing Digital Records

To ensure the ongoing protection of digital records, agencies require efficient and effective means for maintaining, handling, and storing digital records –- both active and inactive -– over time. Policies, guidelines and procedures for the storage of digital records should be an integral component of an agency's digital record keeping framework. There are three ways in which agencies may store digital records -- online, offline or nearline.

· Online – Online records can be contained on a range of storage devices (e.g. mainframe storage, network attached storage or PC hard drive) that are available for immediate retrieval and access. Generally, records stored online will be active digital records – i.e. records that are regularly required for

ministry purposes. Electronic messaging systems and word-processed documents saved to the network server fall into this category.

· Offline – Offline digital records are contained on a system or storage device that is not directly accessible through the agency network and which requires human intervention in order to be made accessible to users. Digital records that are stored offline are usually retained on removable digital storage media (e.g. usb drives, CD, DVD or magnetic tape) and are generally inactive digital records not regularly required for business purposes. Offline digital records may be stored offsite as part of an agency's business continuity plan.

Digital records stored offline are not immediately available for use. Agencies must take responsibility for monitoring and guarding against environmental degradation and changes in technology that may adversely affect the storage media employed.

· Nearline – Nearline storage of digital records means the records are contained on removable digital storage media, but remain relatively accessible through automated systems connected to the network. These digital records are technically considered to be offline. The use of systems such as CD jukebox or magnetic tape silos allow them to be made available through agency networks, in relatively short periods of time and without the need for human intervention (i.e. staff are not required to physically retrieve the storage media on which the required information is retained). Cloud storage also falls into this category.

Generally, digital records will begin life as online records and, as the immediate business need to refer to them diminishes over time, they will be moved to either nearline or offline storage, depending upon the technology available to the agency, the ongoing relevance and value of the records and their retention requirements.

Selecting the Appropriate Storage Method

We strongly recommend that digital records of vital significance to an agency, as well as digital records required for long-term retention within agencies, and digital records of archival value, be stored online.

Online storage devices, such as network storage devices and mainframe storage, have the following advantages.

· Digital records stored online will, in most cases, be retained on the magnetic hard drives that form an agency's core network, where they will be readily accessible to users and can be maintained and controlled as an integral part of the agency's recordkeeping system.
· Large storage capacities allow for significant quantities of digital records to be retained on a single storage device.
· Regular integrity checks of digital records can be more readily performed and, in some instances, it may be possible to automate these tasks.
· Digital records stored online have a greater likelihood of being identified and included within any changes made to agency IT systems, such as system-wide migration processes.
· Online storage devices need not be linked directly to an agency network. Where security concerns, business considerations or other factors warrant, agencies may opt to establish standalone online storage systems.
· Increasingly, online storage systems can support sophisticated automated techniques and redundant designs that aid digital record control, monitoring and backup.

GCAH does not recommend CDs, DVDs, magnetic tape, cloud storage or other removable digital media

formats that are physically maintained but not accessible from active computer systems. Offline digital storage devices are suitable only for storing relatively low-value digital records and are not recommended for long-term digital records, vital records or records identified as being of archival value. Cloud storage has to potential to be hacked through its Internet portals.

TRANSFERRING RECORDS TO THE ARCHIVES

For Digital Files

There are two ways to transfer digital files to the Archives.

The first method is to contact GCAH and make arrangements to access their cloud file management system. This will allow the agency to upload files directly to the storage area without worrying about significant storage limits. Once the storage is complete, GCAH will download the files and place them in the trusted digital depository.

· Those wanting to transfer files will request the digital transmittal app from GCAH. This routine will prepare the files for transmission to GCAH and will create a small text-based file that must accompany the transfer. The app will change and develop over time, but its basic purpose will not change.

· The agency person will contact GCAH and request access to the cloud-based storage files, or if they have access to their own adequate storage space, like Dropbox, then that can be used. Move the files to the storage area and notify GCAH when the upload is complete.

· GCAH will download the files from the storage space and add them (accession) to the Archival holdings. They will send an acknowledgment that the material arrived. The files marked as official copies on the agency's servers must be deleted.

The second method is to contact GCAH and request a usb-based hard drive which will be sent to the agency which will copy the files to the hard drive and return it to GCAH.

· Those wanting to transfer files will request the digital transmittal app from GCAH. It will be sent along with the drive. This routine will prepare the files for transmission to GCAH and will create a small text-based file that must accompany the transfer. The app will change and develop over time, but its basic purpose will not change.

· Move the files to the storage usb-hard drive and return it to GCAH.

· GCAH will download the files from the storage device and add them (accession) to the Archival holdings. They will send an acknowledgment that the material arrived and was safely transferred. The files marked as official copies on the agency's servers must be deleted.

For E-Mail

Contact GCAH and they will use an app to access the specified e-mail accounts and download the specified e-mails. These will be added (accessioned) to the archival holdings. The originals should be

removed from the e-mail box.

If the agency manages its own e-mail server, then it can, if it wishes, withdraw the desired emails from its system in a mbox format and send that to GCAH which will add the material (accession) to the archival holdings.

CONVERTING DOCUMENTS AND RECORDS TO A DIGITAL FORMAT

General Record Types

Working in an office or archives there are many times when a record needs to be converted to a digital format. The appropriate term is to digitize or migrate the document. Below is a list of document types and the type of file to which they should be converted.

Photographs - can be done on a flatbed scanner. Not all scanners are created equal. Check with friends and colleagues to see what piece of equipment they are using.

· Black and white - Preservation copy: 600 dpi, 16-bit depth and save as a TIFF file. This will preserve the maximum amount of information from the original image.
· Patron copy: change to 8-bit and 100-200 dpi (use 100 for website image) and save as a jpg. This produces a compact image that is easy to share but not useable for print publication.

· Color - Preservation copy: 600 dpi, 48-bit depth and save as a TIFF file. This will preserve the maximum amount of information from the original image.
· Patron copy: change to 100-200 dpi (use 100 for website image) and save as a jpg. This produces a compact image that is easy to share but not useable for print publication.

Audio - CDs, cassettes, reel-to-reel you will need a player that connects to your computer. Either your computer will need an audio card with an analog to digital converter built in or you will need to purchase a separate converter as well as software to accept the digitized file

· Preservation copy: 92,000mHz , 24-bit depth and save as a WAV file. This will preserve the maximum amount of information from the original recording.
· Patron copy: save original as a mp3 file

Video-Film, you will need a player that connects to your computer. You will need to purchase a separate converter as well as software to accept the digitized file. In some cases there is specialized equipment for specific formats such as video tapes or 8mm film

· Preservation copy: Save the film as an AVI file.
· Patron Copy: Copy the film as a mpeg file.

Use of PDF

PDF can be used for a variety of file types. It is not as secure as many suppose, there are programs

available which will edit a PDF file. To create an archivally sound PDF file save the file as a PDF/a file type. This ensures that the file will be viewable on almost any computer platform or operating system.

WAYS FOR CONFERENCE ARCHIVES AND LOCAL CHURCHES TO PRESERVE THEIR ELECTRONIC RECORDS

Why Preserve Digital Records?

Considering the problems of technological change, and the potential instability of digital storage media, 'long term' may not be very long. When applied to the preservation of digital records, 'long term' usually means 'greater than one generation of technology'.

Many records have retention periods greater than one generation of technology. It is important that these records are preserved and accessible.

Long-term maintenance is particularly significant for digital records of archival value. Inadequate preservation strategies can render digital records inaccessible and unusable.

Accessibility requirements apply to all digital records, not just those of archival value. Digital records must remain accessible for as long as they are required.

Planning for Technological Obsolescence

Digital records are dependent on various combinations of hardware, software and media to retain their content, context and structure. Archives must ensure that the technology required to render a digital record usable and accessible is available. It is not sufficient to simply retain records in digital format; the records and associated metadata must be in a format that is viewable with current technology.

Computer technology is subject to ongoing technological obsolescence, with both hardware and software quickly becoming outdated as new upgrades and versions come onto the market. This can result in digital records created using older hardware and software becoming inaccessible in their original form after a relatively short period of time.

Archives that retain digital records for the long term should plan for technological obsolescence by ensuring that records can be copied, reformatted, converted or migrated across successive generations of computer technology. Such planning involves considering hardware, software, operating systems and storage devices.

Archives need to consider a number of interrelated software and hardware issues when preserving digital records, including:
· the proprietary, platform-specific nature of many software applications and the likelihood of their continued availability;

· the cost of maintaining access to obsolete formats (including operating system software and licensing fees) for a system no longer in active use;

· the estimated physical and/or commercial life of the media on which digital records and related metadata are stored; and
· the long-term availability of the hardware and operating system platforms needed to access records stored on different types of media.

Techniques for Digital Records Preservation

Some early approaches to digital records preservation relied on storing records in their original format on physical media – much like boxes are used for the storage and protection of paper records. However, magnetic tapes and disks, and optical storage disks (e.g., CDs and DVDs) are manufactured for short-term storage of digital objects, not long-term archival retention. The greatest concern for this method of preservation, in addition to the relatively short life span of digital media, is the obsolescence of the hardware and software used to access the records. Rapid change in the IT industry and the move from science-based development to commercial development of software and hardware systems, has meant that media rapidly become inaccessible. Consequently, this approach to digital preservation has proven to be wholly inadequate and the GCAH strongly advises against this preservation strategy.

The most common techniques for digital preservation can be grouped into three broad categories. Any one or a combination of these may form the basis for an archives' digital records preservation strategy.

Migration - Conversion

Migration relies on a program of constant transferral (migration) of digital records from older or obsolete hardware and software configurations or generations, to current configurations or generations in order to maintain accessibility. This strategy avoids the obsolescence issues of the physical media solution, preserving the functionality of the digital records and enabling users to retain access to the records –- but requires a substantial investment in resources to undertake the repetitive migration work involved. Furthermore, some characteristics of the original data format may not be retained through the migration process and, as a result, users will lose access to characteristics of the source record that may be important to its meaning.

Conversion is the process of transferring digital records from their original data format to a standardized, long-term preservation format (also known as an archival data format). Conversion is also referred to as "normalization", "stabilization" and "standardization".

The conversion process is a form of migration. However, instead of migrating from an outmoded data format to a current data format, the original data format is migrated to an archival data format. Generally, archival data formats are open source, non-proprietary formats that provide greater potential longevity and are less restrictive than proprietary formats. Conversion reduces the need for repeated migrations.

Encapsulation

Encapsulation requires metadata to be bundled with, or embedded into, the digital object. The metadata

allows the record to be intellectually understood and technologically accessed in the future. A viewer is then required to display the records. This packaging of contextual information ensures the integrity and authenticity of records over time. However, there is some risk that important metadata may be overlooked during encapsulation.

On its own, encapsulation cannot preserve digital records. This technique should be used in conjunction with migration or emulation to ensure the ongoing accessibility of the records.

Emulation

Emulation uses software to recreate the digital record's original operating environment to enable the original performance of the software to be recreated on current computer systems. The result is that the original data format is preserved and may be accessed in an environment that allows for the recreation of the original 'look and feel' of the record. The downside to the emulation approach is that the creation of the underlying emulator software is costly, requiring highly skilled computer programmers to write the necessary code. Furthermore, the intellectual property and copyright issues associated with the emulation of proprietary software may undermine the effectiveness and sustainability of the approach.

GCAH's approach to digital preservation focuses on migration and conversion.

Archival Storage of Digital Files

In order for the digital record to be trustworthy it needs to be reliable, authentic, complete, accessible and durable. These are all core values for archivists. This has been the purpose of recordkeeping since the inception of records. Our tasks as archivists is to ensure the trustworthy character of the record over time. We need to set up a storage and preservation system that will convince the researchers of the future that the records we have bequeathed them are trustworthy.

We suggest a three step process.
· Quarantine
· Preservation/Conversion
· Secure Repository

In many respects this is the identical process for physical records which are quarantined in a receiving room upon arrival at the archives, processed and preserved while being re-housed and arranged and then stored in a safe storage area.

Quarantine

Records will be brought into the archives either by the Internet or on some type of media, e.g. CD, DVD or a USB drive. Hopefully a list, or manifest, of the material will have been created as part of the transfer. If not then one needs to be made. On a computer isolated from the rest of the network the contents of the transfer media are checked to confirm that the files received are those that the originator intended to send and all media are checked for the presence of computer borne viruses.
Once a virus check is passed the records are copied to a carrying device, disconnected from the Quarantine network and stored for a period of 28 days. During the 28 day quarantine period, the virus

definitions on the Quarantine network are updated daily.

After 28 days have passed, the carrying device is again connected to the Quarantine network and the data is again scanned for the presence of viruses.
The first thing an archives has to do is to make sure that its records are "clean." Just as we investigate for mold and insects we need to be sure that no damaging viruses are brought into the archives. The 28 day time lag ensures that virus protection will catch up to any new viruses.

Preservation/Conversion

If necessary the records need to be converted to a standard format, either proprietary or an open standard such as openDocument. We recommend conversion for the following reasons.

· Keeping working copies of older generations of PCs , operating systems and software is just not a viable option. The expertise to manage these older systems is huge. Merely finding parts for many of these machines would prohibit this as a workable solution.
· Building software that emulates the older operating systems and software. Again, the expertise to do this would be huge, and costly. Almost all of the older systems are of a proprietary nature and there would be charges and challenges in creating something that worked like an older system.
· Converting the files to a standard format reduces the complexity of the number of file types to deal with. If, and when, that "standard" or "open" file type becomes obsolete, then the associated costs of the next transfer is also less since the conversion is from one file type to and other. If the conversion is well-designed it will have minimal impact on the fixed nature of the record.

So, as the next step once the material has been determined to be virus-free a carrying device is connected to the Quarantine network and taken over and connected to the Preservation network and the individual data files are converted to your selected standard preservation format. The files created by this process should be recorded on a second carrying device for transfer to the Digital Repository.

Secure Repository

The carrying device is connected to the Digital Repository network and the files of the original data are copied to long-term storage arrays. These storage files should be in a secured space, with limited access and a very secure password. Only a few accounts should be on the system. Logs should be kept of who access this system. For general public access to these records, copies should be made and place on the public network. But even these files should be placed on a read-only drive.

File Format Types -First Steps

There are a variety of different file formats. Offices are advised to limit the number of types and the corresponding software that supports them. The more file formats and software in use, the greater chance for loss of information because the files become inaccessible. you consider the file format options available to you, you will need to be familiar with the following concepts:
• Proprietary and non-proprietary file formats
• File format types

Proprietary and Non-proprietary File Formats

A file format is usually described as either proprietary or non-proprietary:

• Proprietary formats. Proprietary file formats are controlled and supported by just one software developer.
• Non-proprietary formats. These formats are supported by more than one developer and can be accessed with different software systems. For example, eXtensible Markup Language (XML) is becoming an increasingly popular non-proprietary format.

File Format Types

Files fall into the following large categories
· Text files. These are files associated with MS Word, Wordperfect and other word processing files.

· Some use proprietary files, such as Word, while other files, ASCII files are used by simple word processors like NoteTab.
· Portable Document File (PDF) is a popular proprietary file type used by Adobe Acrobat
· Graphic files,
Vector based files which store images as mathematical formulas. Most frequently used in architectural files and PostScript files used in publishing. This images can be scaled without distortion;
Raster-based files that store images as a collection of pixels. These are also called bit-mapped images. They cannot be scaled without some distortion;
· Bitmap (BMP) one of the earliest. Low quality files often used in word processing.
Tagged Image Format file (TIFF), widely used in many programs. No compression is used in storing the data;
Graphics Intechange Format (GIF) file, widely used on the Internet;
Joint Photographic Experts Group (JPEG) is mostly commonly found in digital cameras today. This popular file uses compression when storing an image.
· Data files. Files used by database software. Most often today these are relational files, which means the file structure is placed in a type of tabular structure. However, internal structure can vary and the indices which accompany the database are often have a unique structure. Also, the growth of popularity of the XML database adds to the complexity of this general file type.
· Spreadsheet files. Spreadsheet files hold information in a tabular format as well as relationships between the various cells of the tables. These are often proprietary.
· Video and audio files. These files hold moving images and sound. Almost all of the popular formats are proprietary.

WAV files. An audio file which captures sound with little or no compression.
MP3 files. An audio file used most often in portable players and on computers.
MPEG files. A compressed movie file.

When creating or saving files it is always better to use a standards-based file and one which uses little to no compression.

EXECUTIVE SUMMARY

Agencies at all levels of the denomination are creating more and more electronic records. the rapid obsolescence of digital technology, agencies should plan for the long-term preservation of digital records.

2017-2020 Edition

Digital records that are to be retained indefinitely by the agency require preservation to ensure their ongoing accessibility. Because digital records can be easily modified, their security is very important. Agencies should plan for disasters –- loss of digital records can be crippling. Agencies should develop an integrated and comprehensive framework for digital recordkeeping.

First must be sure we understand that we are talking about the preservation of electronic records, not electronic publishing. Electronic publishing is the conversion of an existing document, book or image into a digital format and making it available over the Internet. What is currently happening is analogous to the spat of publishing that took place at the end of the 19th and into the 20th centuries. The papers of individuals were collected and published. Electronic publishing allows the originals to be available for the public and scholars. While this is not necessarily a bad thing, it ties up a significant amount of resources and time in recreating what already exists. In many cases libraries are taking existing documents and just digitizing them. Scholars and Librarians tend to think in subject areas first and so there is a propensity when they do turn to archival material to select material by subject matter and then to publish it on the Internet. They become publishers and researchers instead of dispensers of information.

What we are concerned about is the growing body of material which is born digital and which must be preserved for the future. This calls on us to sharpen our appraisal skills and to develop new ways of managing a large body of documentary material.