# Managing Electronic Records
# Best Practices

**Diocese of Owensboro Archives**

*August 2013*

Computers and other electronic devices create many, if not most, of the records we use today. These records, although electronic in format, are treated the same as records in other formats. Fundamental records management principles apply to electronic records just as they do to paper records.

The technical nature of electronic records makes managing them a challenge. There are a variety of electronic records: email, webpages, word-processing documents, spreadsheets, databases, digital images, video and audio files. They can be stored on optical discs, magnetic tape, diskettes, thumb drives, external hard drives and an increasing number of other media. Electronic records are under constant threat from technological obsolescence – new computers may not have the capability to read outdated hardware and software upgrades may leave older formats inaccessible. A lack of planning can render records inaccessible.

## Organization and Storage

The most effective approach to organizing your electronic records is to have a filing system that mirrors your paper files. Create a series of electronic folders and subfolders on a server, arranged hierarchically from the general to the specific in a series of directories.

For easy retrieval, develop naming conventions that are logical, consistent, and allow sensible sorting. For example, if you create board minutes electronically, use the name of the records series followed by the year and month, indicated numerically so that the files sort in chronological sequence: "Minutes 2005_07" (for single digit months, include the leading 0). Place all meeting minutes in a folder named “Board Meeting Minutes.” Organizing records in a systematic manner will also be of help when the time comes to purge electronic records that have reached the end of their retention period.

Save electronic records on your office’s network drive, not your individual workstation (your “C” drive). If your computer were to crash, these files would be lost. They will be backed up regularly if saved to a network drive.

## Security

In addition to fire, flood, and vandalism, computer users must contend with viruses, hackers and hard drive crashes. You can increase the physical security of computers by locking doors and installing intruder, fire, and water detection systems. In addition, implement and update virus protection software and firewalls, make frequent backups, storing them offsite, and use a system of passwords to protect your information.

## Preservation

The most challenging task in managing electronic records is long-term preservation. Magnetic tape can develop read-errors and optical storage media (such as CDs and DVDs) can fail completely after only a few years, especially if they are not stored in the proper environment. To avoid data loss, refresh media by copying data to a new tape or disc every three to five years.

There are a few strategies to anticipate technical obsolescence. One is to copy electronic records to an eye-readable media such as microfilm or paper. This works best when the functionality of the electronic record is no longer needed.

Another strategy is to maintain data in a standard or non-proprietary ("open") format. These are not likely to change over time so the information should remain readable. An effective but labor-intensive and costly solution is to migrate data periodically to a new software version or system, usually every three to five years. Migration should include the records and their associated metadata (system-generated information about the records such as date of creation, creator, file format, etc.). It is recommended to not use software that is uncommon. By using software that is supported by your office will help guarantee the accessibility of the record.

It is recommended that electronic records to be permanently retained be converted to PDF before transfer to the archives.

## Email

The abundance of email messages has made it vital to control them. Inboxes can quickly fill up with important messages mixed in with unimportant ones. Keep good housekeeping practices, such as folder organization, the timely deletion of old messages that are no longer needed, etc. It is a recommended practice for users to quarterly clean up their inbox by purging emails no longer needed (including purging the "Deleted" folder) and putting into folders emails that need to be retained for a longer period but are not currently needed.

When managing e-mail, follow these simple guidelines:

For **non-business related correspondence**, discard as soon as possible. This would include spam, junk, non-business announcements, personal messages, etc.

For **routine correspondence**, keep only as needed. This would include listserv messages, notes from coworkers, general announcements, setting up meetings, etc.

For **official correspondence**, keep permanently. This would include meeting minutes, correspondence that affects policy, procedure, or personnel, annual reports, etc.

The question arises who is responsible for keeping an email if it is a permanent record? If it was sent by a person within the diocesan offices, the sender is responsible for keeping a copy, not the recipient(s). If the email came from outside the diocese, the recipient is responsible for keeping it.

For email with a permanent retention, there are two possible methods to preserve them:

1. Save the email as a file on the office's hard drive.
2. Print the email and delete the electronic file. If this option is chosen, the transactional metadata (date of message, sender, recipient) and attachments must be preserved when the emails are printed.

Proper use of clear and concise subject lines helps identify the content of e-mail messages and helps index and retrieve e-mail messages stored in folders. Clear, concise subject lines are also a courtesy for the recipient in distinguishing important messages from the sea of unimportant junk, or "spam," mail that a person may receive.