# GUIDELINES FOR MANAGING THE ELECTRONIC RECORDS OF SEPARATED EMPLOYEES

## 1. General

1.1 The Archdiocese of Seattle defines *records* as documents in any format that are made or received in the course of business or pastoral affairs and saved for future reference, action, or evidence. Aside from more familiar paper-based documents, records include word processing files, databases, spreadsheets, instant messages and chats, websites, digital images, video files, websites, and sound recordings. Please consult Archives and Records Management if you would like more information.

1.2 Electronic records storage sources that are subject to these guidelines include:

- Desktop, laptop, and tablet computers
- Servers
- Cell/smart phones
- Instant messaging
- PDAs (personal digital assistant)
- Loose media (CDs, zip drives, etc.)
- Voicemail recorders
- Printers
- Data backups

## 2. Voluntarily Separated Employees

2.1 The computer hard drives and other digital assets of *voluntarily* separated employees (when there is no indication to parish/school administrators that the employee is dissatisfied, hurt, or angry) can be repurposed or destroyed once records contained on them have been reviewed with records retention schedules, and materials with ongoing retention requirements or "Archives" designation have been transferred (migrated) to a network server or external storage device. Please document this process by completing an Electronic Records Migration Form, and keep it on file for three years.

## 3. Involuntary or Contentious Resignations

3.1 Any time there is an involuntary separation or contentious resignation from a position at a parish or school, the institution should be prepared for the possibility of litigation. When this occurs, all

electronic records on the employee's computer hard drives (PC and laptop), external storage devices, optical media, and smart phones should be centralized and preserved until any anticipated or impending litigation has been resolved or the statute of limitations has expired. [Hardcopy records should also be centralized and preserved].

3.2 To ensure the admissibility of electronic records in legal proceedings, prevent any deletions or changes to them by disabling the employee's access to all digital technologies either before or simultaneously with their final meeting with supervisors or administrators. It is also important that no other staff open these files, as doing so can change system generated metadata used for authentication in litigation. Instead, make a copy of the file(s) or folder(s) in a separate location, and provide access to the copy, **not** the original. Laptops and other technology assets should be returned to the employee's supervisor before or immediately after the severance meeting.

3.3 In addition to preserving the electronic records of the subject of the separation or resignation, those of the subject's supervisors and other personnel determined by parish/school administration to be key to any possible future litigation should be preserved in accordance with this policy. Contact the Chancellor for advice in determining which personnel and the extent of information that should be included in the preservation tasks. For guidance on selecting acceptable methods of preserving electronic data and selecting external storage devices for preservation please contact Archives and Records Management.

3.4 All data on mobile smart phones issued by a parish or school should also be retained on a backed up server or external storage device after an employee's involuntary separation. All email communications should be retained, including but not limited to the inbox, outbox, sent mail, trash, and any subfolders and email communications therein.

3.5 Before wiping, repurposing, or disposing of digital technologies, the data contained on them should be migrated to a secure network server or acceptable external storage device. Please contact the Director of Archives and Records Management to schedule this. In highly contentious matters a mirror image should be produced through a specific method of copying that replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive. This will contain all the information in the computer, including embedded, residual, and deleted data. This requires specialized hardware and software and should not be attempted by parish or school staff. If possible, contact Archives & Records Management to schedule this *before* the severance meeting so that a plan can be in place to affect the collection and terminate the employee's access to the data concurrent or immediately after the severance meeting.

3.6 A hold should also be placed on any routine records destruction for the employee's email account. Additionally, email communications produced after the separation by parties identified by the Chancellor's Office and Legal Counsel to be "key" to any anticipation litigation should also be preserved with a hold placed on those individuals' email account's destruction schedule. Contact Archives & Records Management to establish a protocol and method for downloading and preserving various email sources. [Staff should *never* use personal email accounts for parish or school business, as doing so may cause the entire account to be subject to discovery during litigation.]

3.7 It is advisable to conduct an annual audit of software, email services, etc. to prepare for quick implementation of legal holds. Include all departments and entities in the audit. This is important to ensure accurate preservation and to verify that the data can be accessed in the future. For example,

legacy software might also need to be preserved, so that data created using that software can be accessed. Additionally, certain server configurations are not easily reconstructed if the server is turned off.

3.8 Add the following to a departing employee questionnaire or interview:

- Request for a list of electronic assets and location of all electronic records, including email.
- Request for login IDs and passwords for Parish or School systems and applications.
- Confirmation that the employee does not have any confidential, proprietary, or business related records (paper or electronic) in his/her possession.
- Confirmation that the employee did not use personal email services to conduct business on behalf of the Archdiocese of Seattle. If they did, they should be instructed not to access that information until a plan is in place to preserve it and remove it from their possession.
- For highly contentious matters, contact the Chancellor or Director of Archives and Records Management for a "duty to preserve" notice to prepared for the employee at the final meeting.

**4. Data Storage, Migration, and Disposal (Involuntary and Voluntary Separations)**

4.1 *Migration*:

- All transfers by parish or school staff of electronic records from one storage medium to another should be documented using an *Electronic Records Migration Form*.
- For assistance in migrating electronic records to other media please contact the Archives and Records Management.

4.2 *Storage:*

- Electronic records transferred to network servers or external storage devices for the purpose of litigation preservation should be included in the institution's backup processes.
- If stored on a network server, access to these materials should be restricted to the pastor, PAA, or principal. If stored on an external storage device, it should be kept in a locked place with access limited to the pastor, PAA, or principal. This is to preserve confidentiality and to safeguard against spoliation of evidence in legal proceedings.

4.3 *Disposal:*

- Contact the Chancellor or the Director of Archives and Records Management to determine when it is safe to destroy any materials, and then securely delete data on

the computer hard drive. Secure deletion is any method which ensures that deleted data cannot be recovered using system functions or commercially available programs. Examples of computer secure deletion include:

- Using software programs designed for secure data deletion (There are free and low cost programs of this type available on the internet.)
- Reformatting the hard drive (Do not use quick or high-level reformatting, which does not actually delete the data itself)
- Physically destroying the hard drive

- After transferring the data on mobile devices to a network server or external storage device, erase the data from the device by performing a hardware reset to factory settings, and subsequently verifying that the data has been erased by visual inspection.