

# Managing Records: Best Practices

American Catholic History Research Center and University Archives

## Creation

- To help identify both paper and electronic documents in the future, it is a good idea to title your documents and include a creation date, or at least a month and year, as well as your name or initials. Always proofread your documents for spelling errors, grammar, and punctuation before sending it to someone or filing it.
- Do not put anything in a document that you would not want to see displayed in a public venue, either in print or online.

## Retention and Storage

### *Paper Records*

- Remember to keep in mind that it is content, not format, which determines how long a record is retained.
- Consider creating an institutional records retention schedule, or individual schedules for departments. A records retention schedule is a document that sets out the periods for which the organization's records should be retained to meet its operational needs and to comply with legal and other formal requirements.
- Most financial, personnel, and tax records need to be retained onsite for a minimum of 5-7 years before being discarded or archived, depending on the institutional, state, and national retention guidelines.
- Records can be stored in an array of organizational schemes, some of the most widely used system use file folders titled by subject, topic, project name, or by date. The folder titles should be intuitive and easy to recognize so that the retrieval of records as easy as possible.

### *Electronic Records*

- Electronic records should be stored in similar ways as paper records, within hierarchical file structures, or alphabetical topical or subject files.
- They should be routinely purged; just because it is electronic does not mean it will be, or should be, saved forever. Delete records that have no long term legal or historical value, such as outdated multiple versions of documents, draft documents, or material that was only used for reference.
- They should also be routinely backed up, either onto a backup server or an external durable storage device.

## **Preservation**

### *Paper Records*

- Records that are outdated or no longer necessary for day to day operations can be archived. The role of an Archive is to house records that must be saved permanently because of their legal and historical value. This includes material such as annual reports, meeting minutes, vital correspondence, promotion files, search committee files, newspaper clippings, and publications created by the organization.
- Records that are vital to the organization and have long term historical value should be archived.
- Material with no long term historical value (such as requisitions and purchase orders, credit card receipts, and cancelled checks) should be shredded regularly and not archived.

### *Electronic Records*

- Electronic records are hardware and software dependent, which means that they are dependent on specific hardware and software to function correctly. Because of this dependence, electronic records need to be migrated to newer technology roughly every 2-3 years. An example can be documents created in Microsoft Word five years ago, which will need to be migrated to an open format non-proprietary format.
- Migrating electronic material may require keeping outdated computers and software/hardware applications to access older electronic records.

## **Access**

### *Paper Records*

- Paper records that are used in the day to day operations of the organization should be stored in secure environments where only staff members, or a limited number of staff members, have access to the records.
- Personnel records and financial records should be stored in locked filing cabinets to make sure that the personal identification information on these records, such as social security numbers, are not widely accessible.

### *Electronic Records*

- To keep sensitive electronic records secure, it is necessary to store them in password protected computers, secure databases, and depending on the situation, the use of encryption software may be helpful.
- Access to electronic records in the long term will require proper management, storage, and migration.
- It is important to limit access to vital electronic records to approved personnel because changes to electronic records can be made very easily, and it is important to be able to prove the authenticity of the record.

5/28/2014