THE CHURCH OF ENGLAND

RECORD CENTRE

Records management toolkit

Looking after your electronic records

Summary

This factsheet intends to explain how to manage documents created and stored on a computer. You will discover:

- How to create high quality electronic records and what formats to use
- How to name folders and files
- How to store electronic records so that your data is secure
- How to destroy and archive electronic records

The guidance which follows is not prescriptive and should be adapted wherever necessary to meet local circumstances.

Introduction

The advice below should be read in conjunction with the factsheet “Organising your records”, which gives advice on setting up a filing structure for your records. Having a well thought out filing structure is the basis of managing your records well, whether you are dealing with paper or electronic records. This factsheet gives some specific tips about how to manage electronic records across their life cycle.

Creation of electronic records

Electronic records are created in one of two ways:

- Electronic records may start off as paper records and be converted into electronic records by scanning them. For example, many modern photocopiers can be used to scan documents into PDFs.
- However, most records are “born electronic” – that is, they are created on computer in the first place.

In either case, the electronic record will need to be given a clear file title and saved in the correct place.

Creating electronic records by scanning paper documents

In some situations, scanning of paper records may be done on a routine basis and the original paper record destroyed. This might make sense if most other information on the same subject is filed electronically or if the records need to be accessed remotely (for example, a diocesan bishop’s office could decide to scan letters and store them electronically so that area bishops can access the scanned copies in their own offices).

However, in most cases the routine scanning of records is time consuming and is not particularly cost effective. Many records will only be retained for a limited period of time and used infrequently during the period they are held. In such cases the time and effort spent scanning documents will be disproportional to the benefit of having an electronic version to hand. Before embarking on a scanning project, it is always sensible to do an informal time and motion study to see how long the scanning process will take compared to the potential time saving in accessing the scanned record. This will usually involve scanning documents on a trial basis. Before destroying any original documents, it is also worth considering whether the original records are of archival value. Diocesan Record Offices (DROs) will not necessarily be able to accept electronic records, so the long term retention of your records might be in jeopardy.

Creating electronic records on computer

Many records which are “born electronic” are word processed documents, including letters, memos, minutes and reports. Electronic records also include spreadsheets and databases, but these records tend to be continually updated rather than recording a particular transaction at a particular time.

It is important that word processed documents are created using a **consistent layout**, so that documents of the same type look the same. This may be achieved by:

- Using document templates for particular types of documents.
- Ensuring that fonts and paragraph spacing are consistent. If using Microsoft Word, the use of Word Styles is strongly recommended.

Documents should generally include the following information on the first page:

- A **clear title or subject line** – this can be included as a “Re:” line on a letter.
- A **clear date** – but if inserting the date in Microsoft Word do not tick the “update automatically” option, as today’s date will then be shown whenever the document is opened (rather than the date when the document was actually created).
- A **version number** in cases where a document goes through a number of changes and the earlier copies are retained. Version numbers can be of two types:
  - Version 2, Version 3 etc – where a major revision is made
  - Version 2.1, Version 2.2, Version 2.3 etc – where a minor revision is made
- The **author** or the department creating the document.

It is also helpful to add page numbers to documents. Page numbers are particularly valuable when long documents are printed out.

Initially, the document will probably be saved in the same **format** in which it is created. For example, a document created using Microsoft Word will normally be saved as a Word document. This is fine for documents which only need to be retained for a limited period of time (say 10 years). However, in the long term such proprietary formats carry the risk that the record will no longer be readable, as the software required to access the file may have become obsolete. You might consider using the following formats for documents you need to retain for a long period. However, it is important to stress that there are many unanswered questions over the issue of digital preservation and so any decision or strategy proposed must be carefully investigated and planned to ensure it is the correct decision for your place of work and the records in question:

- Word processed documents may be saved as text files or PDFs. Text files preserve the text of the document but not the formatting, whereas PDFs preserve the appearance of the original document. Text files are, however, a particularly stable and reliable data preservation format.
- Excel documents can be saved in comma-separated values (CSV) format. This effectively saves the spreadsheet as a text file, with each new line defining a row, and commas separating the values in each column. It should

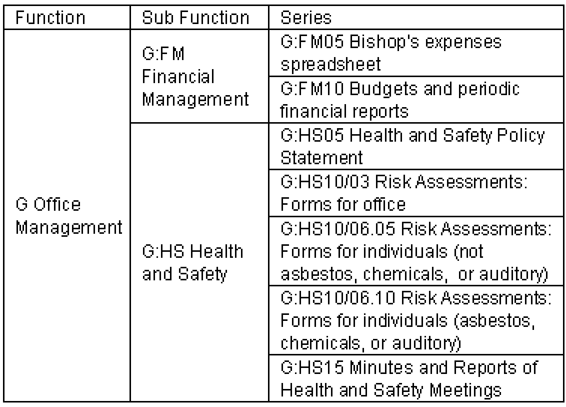
be noted that some information, such as the formulas used to make calculations in the spreadsheet, will be lost by saving in CSV format.

As described in the factsheet on “Looking after your paper records”, printing to paper is another option for preserving documents of long term value that are “born electronic”. Whilst paper is a format which has a proven track record in withstanding the test of time, it is still important to remember that it should be correctly managed to ensure its long term preservation. The factsheet “Looking after your paper records” gives further details.

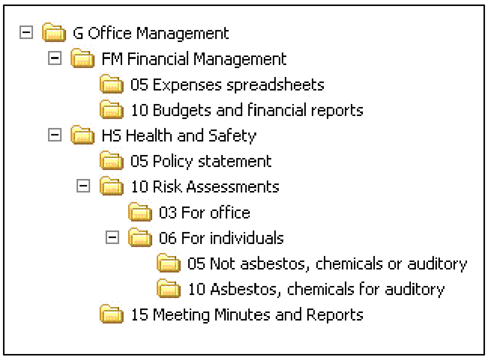
Naming files and folders

All documents stored on computer are called “files” and are stored in “folders”. Both files and folders should be carefully named and organised to ensure that records can be easily managed and retrieved.

Folders should be organised into a hierarchy based on your filing structure. The factsheet “Organising your records” gives advice on designing a filing structure for both paper and electronic records. It is important that folders are named strictly in accordance with the names in your filing structure. Any codes should be included in the folder name, with the folder name starting with the code. This ensures that folders which are at the same level in the hierarchy are listed in the right order. Folders should be nested to form a tree structure, creating folders within folders to reflect the hierarchy. The example below demonstrates how part of a filing structure could be made into an electronic folder structure:



Function	Sub Function	Series
G Office Management	G:FM Financial Management	G:FM05 Bishop's expenses spreadsheet
		G:FM10 Budgets and periodic financial reports
	G:HS Health and Safety	G:HS05 Health and Safety Policy Statement
		G:HS10/03 Risk Assessments: Forms for office
		G:HS10/06.05 Risk Assessments: Forms for individuals (not asbestos, chemicals, or auditory)
		G:HS10/06.10 Risk Assessments: Forms for individuals (asbestos, chemicals, or auditory)
		G:HS15 Minutes and Reports of Health and Safety Meetings



- ⊟ G Office Management
  - ⊟ FM Financial Management
    - 05 Expenses spreadsheets
    - 10 Budgets and financial reports
  - ⊟ HS Health and Safety
    - 05 Policy statement
    - ⊟ 10 Risk Assessments
      - 03 For office
      - ⊟ 06 For individuals
        - 05 Not asbestos, chemicals or auditory
        - 10 Asbestos, chemicals for auditory
    - 15 Meeting Minutes and Reports

Points to note include:

- The file codes define the tree structure of the folders, with each new element of the code indicating the need for a new sub-folder. For instance, in the example above the group of file series starting “G:HS10” show that a folder is needed called “10 Risk Assessments”, within the folder “HS Health and Safety”. Sub-folders are then needed to distinguish between office risk assessments (03) and risk assessments for individuals (06). Finally, another level of sub-folder is required within “06 individuals” to distinguish between those risk assessments that are not related to asbestos, chemical or auditory matters (05) and those that are (10).
- It is not necessary to include the full file code at each level of the structure, just the part of it not shown by the folder above. Similarly, it is also possible to abbreviate file titles where the folder structure already gives a context. For

instance, "HS.05 Health and Safety Policy Statement" can become "05 Policy statement" in your folder structure.

- It is likely that you will add further folders underneath the folders which are set out in your filing structure. For instance, within the folder for budgets and financial reports it would be sensible to have separate folders for each budget year.

Files should be carefully named so that the combination of file and folder name clearly indicates the contents. It is helpful to establish a series of naming conventions for particular types of documents. For example:

- Minutes – meeting date in a recommended format (yyyy mm dd) and name of the group or committee, for example "2011 08 01 Diocesan Advisory Committee Minutes" rather than "1 August.doc". Having year then month in number format in the file title means any file list on screen will be in a helpful and logical order.
- Reports – date of report (in yyyy mm dd format), name for report and version number if applicable. For example, "2011 09 14 Diocesan Communications Strategy v5.6.doc".

The following general points also apply when naming files and folders:

- Is there a recognised term for the subject? Use this in preference. Folder names should be the same as those used in your filing structure.
- Is the term likely to be recognised in the future? Try not to use current buzz words which may have passed out of use in the future when the folders have not. For the same reason, try not to use abbreviations unless they are very obvious.
- If the subject is highly sensitive, for example an investigation into child abuse, files and folders should be very carefully named. Whilst someone may not be able to access the record through security controls, if they are able to see the name, it could give enough sensitive personal data to expose your office to problems and potentially endanger the named individual.
- It is worth considering adding the filename and filepath to the footer of every document you create once it has been saved, to enable anyone with a paper copy to identify what it is and where the electronic copy can be found.

Storage and security of electronic records

The greatest risk to your records is misplacement, loss and unauthorised access. Consequently it is vital that you properly control access to and use of your records, whether they are held on in-house computer systems or in outsourced storage.

Storage of electronic records on in-house computer systems

In most cases electronic records will be stored on in-house computer systems. While parishes may rely on a single stand alone computer, most dioceses, bishops' offices and cathedrals will have a computer network with file storage on a central server. This may be supported by an **Electronic Document and Records Management System (EDRMS)**, which is a specialist piece of software to manage electronic records in a shared network environment. If an EDRMS is in place, there should be clear procedures for its use. An EDRMS will only improve electronic records management if it is correctly used. It should be supported by a developed filing structure, along with clear procedures and practices for users to adhere to, including arrangements for regular maintenance.

In the absence of an EDRMS, the next best alternative is to store records on a **shared network drive**. This is far better than saving documents to a personal file space such as “my documents”, as records can readily be accessed by colleagues when required – better one copy in a shared drive than several all in personal drives or folders. Where necessary, access to shared folders can be limited to those who have a need to use the contents. This can be done on a folder by folder basis on the network drive. The alternative of password protecting individual documents to restrict access is not recommended, as passwords can cause serious problems if users lose them, leave or are away for a protracted period of absence. In these circumstances it is almost impossible to recover the contents.

It is essential to make regular **backups** of your data, so that data may be restored following a disaster or the accidental deletion or corruption of data. Backups should be stored securely away from the location of the machine or system on which they were created, ideally in another building or at least in a different room in the same building. A parish may decide to buy an external hard disk drive, which are quite cheap and simply plug into a USB port. The disadvantage of this method is that you will have to actively remember to make a backup, so an alternative is to set up automatic backups via the free or cheap online storage offered by many broadband and email providers (see section on outsourced storage below). In larger offices, such as dioceses, the backup procedure will usually be managed by the IT department. However, the backup will only cover network drives – documents stored on local drives (such the <C> drive) are not backed up and are not secure!

The use of **portable storage devices** such as USB memory sticks should be strictly limited and avoided altogether for storing sensitive information (for example, names and addresses). This is because:

- They are easy to lose. If a USB drive goes missing there is a risk that it will get into the wrong hands. This can be highly embarrassing or worse still, jeopardise the security of those individuals whose details are contained in the data on the memory stick.
- They can easily corrupt and become unreadable as their manufacturing quality varies greatly.
- They are a major transmitter of computer viruses. If a machine they are plugged into has a virus, it can be transferred to the USB drive, which if plugged into another network can transmit a virus behind a firewall.

Outsourced storage of electronic records

An increasingly popular option is to outsource computer services and file storage to an external provider. Sometimes known as “cloud computing”, both computer applications and files may be accessed via the internet. This can be an inexpensive way of obtaining computing services and providing a backup solution for your files, but there are associated risks. For example, it is important to be clear about what would happen if a company providing external file storage was to cease trading. It is recommended that these sorts of issues are looked at in detail before deciding to outsource storage of electronic records. This particularly applies to records for which no paper copy is held.

Destruction and archiving of electronic records

As with paper records, most electronic records should be **destroyed** after an appropriate time period, rather than being stored indefinitely. Just like paper storage, electronic storage costs money and there is the added complication of making sure that the records remain readable as new software is adopted.

The retention advice given in separate factsheets for parishes, dioceses, bishops' offices and cathedrals gives guidance on how long to keep particular types of records. Deleting information from computers is, of course, relatively easy compared to destroying paper records. However, simply deleting a file will not necessarily prevent it from being recovered by an expert user. Before throwing away any computer hardware it is therefore important to completely clear the hard drive, and (for added security) physically destroying it. A computer expert will be able to advise.

You must remember that as part of any backup procedures you have in place there must be provisions for the deletion (or overwriting) of your backups. If you regularly delete files from your network drive to ensure compliance with a retention schedule, but then fail to delete backups you will be inconsistent in your approach to retention management. Consider how long it is necessary to maintain your backups for and then put in place a continual cycle to regularly delete or overwrite the data. Again, in larger offices this will be handled by the IT department.

It may be appropriate to retain some electronic records as **archives**. At present, electronic archiving is still in its infancy and most Diocesan Record Office (DROs) are not set up to receive electronic records in the same way as they receive paper records. Nevertheless, advice should be sought from the DRO, preferably at the time when the records are being created. Details of the DRO for each diocese are given in the Church of England yearbook (there may be more than one DRO for some dioceses). Further information on DROs is available in the factsheet "Agreements with record offices".

Factsheets available in the records management toolkit

- What is records management
- Organising your records
- Looking after your paper records
- Looking after your electronic records
- Looking after your emails
- Looking after your multimedia records
- Agreements with record offices
- Access to records
- Data protection
- Copying and copyright
- Glossary

Further guidance

For further guidance please contact the Church of England Record Centre:

15 Galleywall Road, South Bermondsey, London, SE16 3PB.

020 7898 1030

archives@churchofengland.org

Last updated January 2013