

Records Management Guidance for Synods and Churches

Contents

What is Records Management?	1
Why is Records Management Important?.....	1
The Records Lifecycle	2
Record Creation	2
Storing Records.....	3
Appraising Records	5
Final Action: Destroy or Transfer to Archives.....	5

What is Records Management?

Records management is the methodical control of an organisation's records from their creation to disposal in order to meet business needs, statutory and fiscal requirements, and to identify records with archival value.

The URC's records are any recorded evidence of its activities created or received in the conduct of its business. These records can be electronic and paper, and include Word documents, Excel spreadsheets, databases, emails, photographs, letters, signed minutes etc.

Why is Records Management Important?

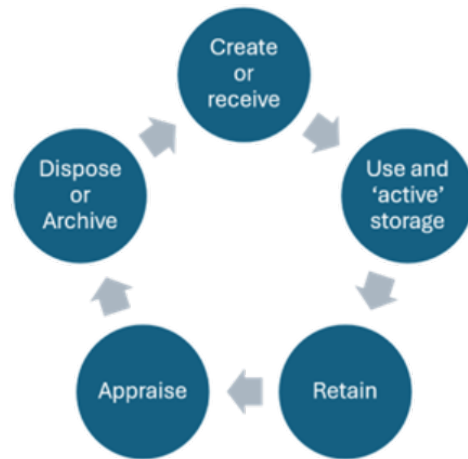
- **Quick access to information** – Records management helps us find accurate and reliable information quickly, ensuring the right people can access the right information when they need it.
- **Saves space** – Keeping records only for as long as they are needed frees up valuable physical and digital storage space.
- **Preserves history** – It helps identify records with historical value, ensuring the history of the Church is preserved for future generations.
- **Supports sustainability** – Deleting records that are no longer required reduces unnecessary storage and helps lower our environmental impact.
- **Ensures legal compliance** – Records management helps the Church meet UK legal requirements by keeping records for the correct length of time and disposing of them appropriately.
- **Protects sensitive information** – It identifies records containing confidential or personal information and ensures they are stored and handled securely.

The Records Lifecycle

The Records Lifecycle helps us understand the different stages a record goes through, from when it is created to when it is destroyed or preserved in an archive. Understanding these stages helps us manage and care for records appropriately throughout their life.

The stages of the records lifecycle are:

1. Create or receive
2. Use and 'active' storage
3. Retain
4. Appraise
5. Dispose or Archive



While records are actively used, they should be created, stored, and managed properly so they can be found easily when needed and kept secure. When they are no longer in active use, they should be dealt with in line with the Retention Schedule, either through secure destruction or transfer to a local archive service for permanent preservation. These stages will be explained in more details in the following sections of this guide.

Record Creation

When creating records, you should:

- 1. Create reliable records:** Records should accurately reflect what was communicated, the decisions that were made, and the actions that were taken. Information should be complete, trustworthy, and able to serve as evidence of business activities.
- 2. Create records when they are needed:** Records should be created to document important activities, transactions, decisions, and events. This is particularly important where there are legal, regulatory, operational, or historical requirements to maintain evidence of what occurred.
- 3. Use clear titles and dates:** Every record should have a meaningful title and an accurate creation date. Titles should clearly describe the content of the record so that it can be easily identified and retrieved. Where possible, the title and date should also appear within the document itself, for example in a header or footer, to ensure they remain visible if the record is printed or shared separately from its original location.
- 4. Fix records once they are complete:** During drafting and review, documents are subject to change and are not yet considered final records. Once a document has been approved, completed, or otherwise captured as a record, its content should be fixed and protected from further alteration.
- 5. Apply version control where required:** If changes are needed after a record has been fixed, the amended content should be saved as a new version rather than overwriting the original.

Version numbers, such as *1.0*, *1.1*, or *2.0*, help distinguish between major and minor changes. Labels such as *Draft*, *Final*, or *Final Approved Version* can also assist users in identifying the current status of a document.

Storing Records

When records are no longer in active use, they may need to be retained for a period before disposal. During this time, they must be stored securely to protect them from loss, damage, unauthorised access, or alteration, and to ensure the URC can meet its legal and operational obligations.

Maintain an inventory

Whether records are physical or electronic, it is very important to keep an up-to-date list of what you have. This can be maintained in whatever format is most practical, such as a spreadsheet, database, document, or paper register. The inventory should include key information such as the record title, date of creation, storage location, retention period, and the final disposal action required once the retention period has expired. This will help ensure records can be located, managed, and disposed of appropriately.

Paper Records

When storing paper records, you should:

- **Store records only on church premises**
Records should be kept in designated church locations and not in private homes, unless there are exceptional circumstances and appropriate authorisation has been given. This helps ensure records remain secure, accessible, and under organisational control.
- **Use suitable storage containers**
Records should be stored in appropriate boxes, filing cabinets, or shelving units that protect them from damage and help keep them organised and easy to retrieve.
- **Choose an appropriate storage environment**
Storage areas should be as secure and fire-resistant as possible, well ventilated, and free from damp, mould, excessive heat, and direct sunlight. Locations should also be protected from flooding, insect infestations, and rodent activity. As a result, areas such as attics, basements, garages, and outbuildings are unsuitable for long-term records storage.
- **Protect records from unauthorised access**
All records should be safeguarded against unauthorised viewing, alteration, or removal. Confidential, sensitive, or particularly important records should be stored in locked cabinets, secure rooms, or safes.

Electronic Records

As more records are created and maintained in digital formats, it is important to ensure they are stored securely and remain accessible for as long as they are needed. Electronic records should be managed with the same level of care as paper records. They should be organised within a structured filing system, retained for the appropriate period, and securely disposed of when no longer required. When managing electronic records, you should:

- **Keep software and systems up to date:** Install software updates, security patches, and antivirus updates regularly.
- **Protect sensitive and personal information:** Records containing confidential, sensitive, or personal data should be protected against unauthorised access. Appropriate safeguards may include access controls, password protection, encryption, and secure methods for sharing files.
- **Secure devices when not in use:** Computer equipment should be protected from theft, loss, or unauthorised use. Devices should be locked when unattended, stored securely when not in use, and not left in locations where they may be accessed by unauthorised individuals.
- **Maintain good file management practices**
Keep filing structures organised and logical, review folders regularly for duplicate or obsolete material, and ensure records can be easily located when needed. Consistent naming conventions and effective version
- **Store records on Church-owned devices or approved systems:** Records should be saved on Church-managed computers, servers, or approved cloud services. Records should not be stored on personal devices, personal email accounts, or unapproved storage platforms.
- **Follow the 3-2-1 rule:** Maintain three copies of important records, stored on at least two different types of media, with one copy kept off-site or in a secure cloud-based service. For example, records could be stored on a Church computer, backed up to an external storage device held in a separate location, and copied to an approved cloud storage service.
- **Back up records regularly:** Backups should be carried out routinely to ensure all copies remain up to date and that records can be recovered if data is lost or corrupted.
- **Check records periodically:** Digital records should be reviewed at least annually to confirm that files can still be opened, accessed, and read using current software and systems. This helps identify any issues before records become inaccessible.
- **Consider paper copies for critical records:** Where there are concerns about long-term digital preservation, particularly for records of enduring value, a paper copy may also be retained as an additional safeguard.

What about emails?

Emails can provide important evidence of decisions, actions, transactions, and communications, and may need to be retained for legal, regulatory, operational, or historical purposes. However, large volumes of unmanaged email can make it difficult to find important information.

Emails should be reviewed regularly and managed in accordance with the retention schedule. Good email management practices include:

- Delete transitory emails such as out-of-office replies and routine acknowledgements when no longer needed.
- File short-term emails (e.g. meeting notices and event arrangements) in appropriate folders and delete them when obsolete.
- Save important emails as records if they document decisions, actions, or other significant Church business.
- Save emails with long-term value in an approved format or print them and transfer them to your local authority archive service for permanent preservation.

Appraising Records

When a record reaches the end of its retention period, you need to decide what should happen to it next. There are usually two options:

- Confidential destruction if the record is no longer needed.
- Transfer to an archive service if the record has long-term historical value and should be kept permanently.

How do you decide?

The Records Retention Schedule explains:

- How long different types of church records should be kept.
- When records can be destroyed.
- Which records should be offered to the local public record office to become part of the church's archive.

You should always use the Records retention schedule to appraise records and can find it within the URC Resources Hub.

Top Tips for Appraising Records

- **Always follow URC guidance:** Use retention schedules, collecting policies, and appraisal guidance to help you make consistent decisions.
- **Focus on the information, not the format:** For example, emails are not kept just because they are emails. They are kept if they record important decisions, activities, or events.
- **Don't keep records just because they are old:** Age alone does not make a record valuable.
- **Seek advice from others:** Record creators and subject experts can often help you understand the importance of a record.
- **Check for duplicates:** Keep the best or most complete version and remove unnecessary copies.
- **Keep records that tell the church's story:** Documents that show important decisions, activities, and achievements are often the most valuable.
- **Most importantly, ask if you're unsure:** If you are not sure whether a record should be kept or destroyed, set it aside and seek advice from the URC Archivist and Records Manager before making a decision.

Final Action: Destroy or Transfer to Archives

Now you have appraised the records and determined their final action, you must follow a process to ensure that it is undertaken correctly.

Destroy

When records have reached the end of their retention period and are no longer required, they should be disposed of securely to protect confidential, personal, and sensitive information.

Paper Records

- Use **confidential shredding** for records containing personal, financial, or sensitive information.
- Place records in approved confidential waste bins for collection by a secure destruction company.
- Ensure records are shredded or destroyed so that information cannot be reconstructed.
- Obtain and retain a **certificate of destruction** where appropriate.

Electronic Records

- Delete records from shared drives, personal drives, email accounts, and business systems when authorised to do so.
- Empty recycle bins and deleted items folders where necessary.
- Ensure records are removed in line with organisational procedures and data protection requirements.
- For storage media such as USB drives, CDs, DVDs, and hard drives, use approved methods of secure wiping or physical destruction.

Before Disposal

Always check that:

- The retention period has expired.
- There is no ongoing legal, audit, safeguarding, or operational requirement to keep the records.
- The records are not required for permanent preservation as part of the archive.
- Disposal has been authorised in accordance with the Records Retention Schedule.

Remember, records containing personal or confidential information should **never be placed in general waste or recycling bins**. If you are unsure whether records should be destroyed or archived, contact the **URC Archivist and Records Manager** for advice before taking action.

Where to deposit archives

The URC advises all churches to deposit their archival records at their local public record office. Records will be looked after by professional staff, safeguarded for the future and catalogued and made available to researchers.

If a church has not already deposited records with their local public record office, they should contact them to discuss the possibility of transferring records.

Archive deposit agreements

Before transferring records to a local archive or record office, it is good practice to agree the terms of the transfer in writing, this is known as an Archive deposit agreement. Points to consider include:

1. **When to transfer records:** Records should be transferred when they are no longer needed for current business. Regular transfers, such as every 5–10 years, are often easier to manage than occasional deposits.
2. **Loan or gift:** URC records should always be deposited as a **Loan** to local record offices, as this ensures ownership is retained by the Church. Local Record Offices may request that records are transferred as a gift, meaning that they own the records. If this is requested, **please contact the Archivist/Records Manager before transferring any records**.
3. **Access to records:** Discuss how and when the records will be made available to researchers, particularly if some records need to remain closed for a specified period.
4. **Data protection:** Speak to the archive service about how records containing personal or sensitive information will be managed and protected in line with data protection requirements.

Preservation tips

To help ensure records remain in good condition for long-term preservation:

- Use brass or plastic paperclips instead of metal paperclips, pins, or staples, which can rust and damage documents.
- Avoid using rubber/elastic bands, as they deteriorate over time and can damage paper.
- Take care with plastic folders and wallets, as some plastics can stick to ink and damage documents. Where possible, do not store records in plastic pockets, as these need to be removed before records can be archived.
- Handle records carefully and keep them in a clean, dry environment away from damp, heat, and direct sunlight.

Archiving the church's website

The [UK Web Archive](#) offers an easy way for churches to archive their website. The Web Archive takes six monthly 'snapshots' of a website and makes them available via its website for free. The main URC website and several church websites are archived in this way.

For more information, contact the Web Archive using the [form on their site](#).