The Coventry Diocesan Board of Finance

DATA RETENTION POLICY

Document Overview

Purpose	The purpose of this policy is to ensure that all staff and volunteers are aware of their responsibilities in maintaining records and record keeping systems in accordance with the regulations and as required in the CDBF Data Protection Policy.
Confidentiality	This document is not confidential.
Document owner	Stephen Davenport, Data Protection Officer
Status note	Final
Distribution	All DBF staff, Clergy (who work within the CDBF systems), Trustees and Volunteers
Required action	Publish.
Proposed next step	

Version History

Version	Date	Status Note
1.0	11/03/2025	Final
2.0	03/07/2025	Church of England guidance and links updated

1. Introduction

1.1. The Coventry Diocesan Board of Finance recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the organisation. This document provides the policy framework through which this effective management can be achieved and audited.

2. Scope of the Policy

2.1. This policy applies to all records created, received or maintained by DBF staff and volunteers in the course of carrying out their functions.

2.2. Records are defined as all those documents which facilitate the business carried out by the CDBF and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

3. Responsibilities

3.1. The organisation has a legal responsibility to maintain its records and record keeping systems in accordance with the regulations.

3.2. The Data Protection Officer will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

3.3. As stated in the CDBF Data Protection Policy, if you are an employee, any breach of this Data Protection Policy may result in disciplinary action. If you are a non-employee, any breaches of this Data Protection Policy may result in us terminating your contract with immediate effect.

3.4. All CDBF staff and volunteers (including Joint Workers) and Officers (e.g. Archdeacons and clergy) who are responsible for Processing Personal Data, or who supervise such Processing undertaken by diocesan officers, trustees and/or volunteers, are responsible for ensuring all Personnel comply with the CDBF Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.5. Individual employees and volunteers must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the CDBF Retention Policy and Church of England's records management guidelines.

4. Relationship with Existing Policies

4.1. This policy has been drawn up within the context of the:

- CDBF Data Protection Policy
- CDBF Privacy Policy
- CDBF Data Breach Protocol

- CDBF Subject Access Request Procedure
- UK General Data Protection Regulations (UKGDPR)
- Church of England – Guide to the Church of England Retention Schedule (2025)
- Church of England – Personal Files Relating to Clergy (May 2018)
- Church of England - Records management toolkit Safeguarding Records - Retention (December 2015)
- Chartered Institute of Personnel and Development (CiPD) Retention Periods Guidance (Appendix 1)

5. Safe Disposal of Records

5.1. Where records have been identified for destruction, they should be disposed of in an appropriate way.

5.2. When destroying personal data, paper documents will be shredded and CD-ROMs will be physically destroyed or disposed of professionally. (The IT Systems Manager should be consulted when destroying any electronic data.) When personal data is not required it should also be deleted from Trash/Deleted Items folders to prevent recovery.

5.3. Any other records, such as hard drives should be disposed of in other appropriate ways. There are companies who can provide confidential waste bins, shredding and other services which can be purchased to ensure that records are disposed of in an appropriate way (Please speak to the Director of Operations or IT Systems Manager to arrange this).

6. Transfer of Information

6.1. Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

7. Retention Guidelines

7.1. The CDBF will adopt and follow the Records and Information Management Guides from the Church of England and the CiPD Guidance (Appendix 1).

7.2. The records management guides have been researched and produced by records and archive management specialists at the National Church Institutions. They have used expert advice from the National Archives, local record offices and the wider records management and archive profession. Input has also been received from over 70 users from across the Church.

7.3. The guides are designed to help parishes, dioceses, bishops and cathedrals develop a consistent and best practice approach to looking after church records in their care, whether paper or electronic.

7.4. The guides are being reviewed and updated, and new guides will be published when they have been produced.

7.5. The CiPD Guidelines (Appendix 1) introduces the legal position on the retention of HR records in the UK, including the Data Protection Act 2018, the UK General Data Protection Regulation (UKGDPR) and the employment practices code. It offers two checklists: one giving statutory retention periods for information

where these exist, and the other giving recommendations for keeping information such as application forms or parental leave information.

7.6. Where guidelines are not provided for particular categories of data, the CDBF will provide these as part of this policy.

7.7. These guidelines are designed to help diocesan officers to distinguish between the different kinds of records and decide how long and where they need to be kept. The retention periods given in these guidelines are based on either on legislation or on recommended good practice. These guidelines should be applied to all records whether in a traditional paper or in an electronic format.

Guide to the Church of England Records Retention Schedule

7.8. Introduction

This records retention schedule (published in 2025) replaces the previous guides on retention, including: Keep or Bin, Cherish or Chuck, Chapter and Verse, and Save and Delete.

7.9. What is a retention schedule?

It is a document that sets out how long records should be retained for, and the justification for that retention and what the disposal action should be.

7.10. Why should we use this schedule?

The schedule has been developed in consultation with a range of stakeholders from across the Church of England. It provides best practice for applying retention and disposition of records held by church bodies.

- It is far more comprehensive than the previous schedules
- It provides defensible reasons for retaining, archiving and destroying records
- It should give you confidence that you can destroy records at the appropriate time
- It supports the requirements of Data Protection Legislation
- It supports good record keeping practices

7.11. Why is there only one schedule when previously there was four?

To bring a consistent approach and avoid duplication of information and therefore disparity between the different church bodies.

7.12. Who should use this schedule?

This records retention schedule is primarily designed for use by the following: Cathedrals, Minsters, Bishops Offices, Diocesan Offices (Including DBF's DBE's), Archdeacons, Deaneries, and Parishes of the Church of England. However, many of the items within the schedule can be applied by other Church bodies not listed.

7.13. There is clear guidance on how files and emails should be named and stored to ensure they can be found easily if needed for auditing purposes or in the case of a Subject Access Request.

7.14. All staff and employees must read this document and follow the guidance that relates to their area(s) of work.

Church of England – Personal Files Relating to Clergy

7.15. This guidance is designed to assist bishops in managing personal information about the clergy for whom they are responsible, and to promote good and consistent practice in record keeping. It considers the requirements of data protection legislation and the law of confidentiality, and also addresses practical issues of file management.

7.16. The guidance deals only with personal files about clergy ("clergy personal files", also commonly known as "blue files"). It does not cover personal files relating to readers and other licensed lay ministers, although the same general principles apply to these. Nor does it cover files relating to those who are exploring a vocation to

ministry or who are in training but not yet ordained. Ministry Division issues guidance to Diocesan Directors of Ordination about record keeping in this context.

7.17. The Bishop is the Data Controller of all clergy 'Blue Files', these are held at Bishop's House. All personal information about clergy must be held together in one place and be managed by the diocesan bishop and his staff, although in larger dioceses it may be necessary for suffragan bishops to hold the personal file of those clergy for whom they are responsible.

7.18. Those staff who contribute information to clergy personal files (for example, archdeacons and HR) need to be clear about where the file of any cleric is kept and the arrangements for keeping it updated. They should not keep separate files (other than day to day working papers), and where this is the case a note should be placed on the file to indicate that material is held elsewhere and to explain how it may be accessed. Such working papers should be transferred periodically to the main file: each diocese should have in place a policy to ensure that this happens regularly and systematically.

Records Management Safeguarding Records - Retention

7.19. For the purpose of this guidance safeguarding records includes:

- **Allegations/Concerns**: Any information that relates to allegations of abuse by church officers1 or Any information that relates to a concern around a risk of potential harm to a child or adult e.g. referral information, advice and guidance offered to Parishes, case files and records
- **Risk Assessments:** Any information that relates to risk assessments and managing risk in church settings
- **Employment:** Any information that relates to the recruitment, support and training of clergy, church employee's and church workers in line with Safer Recruitment Practice Guidance (including information from the Disclosure and Barring Service)
- **Discipline:** Any information that relates to disciplinary action in relation to a member of the clergy/church officer or employee e.g. clergy personal (blue) files, supervision files, personnel files, clergy discipline measure, legal aid
- Any information that relates to the safeguarding leadership and governance and development of local safeguarding practices and policy e.g. minutes of safeguarding panel, policy development, minutes of Diocesan Synod, training deliver records, Quality Assurance processes and outcomes etc.

7.20. **PLEASE DO NOT DESTROY ANY PAPERWORK OR FILES RELATING TO SAFEGUARDING WITHOUT SPEAKING TO AND OBTAINING PERMISSION FROM THE DIOCESAN SAFEGUARDING ADVISER FIRST.**

8. Data Retention Tables

8.1. Data Retention Tables have been created for all departments. These can be found in *Common Files - Staff Info\Diocese\Data Protection and IT\Other Information*. These have been created in line with the Records Management Guides from the Church of England and the CiPD Guidance (Appendix 1).

8.2. All staff are required to manage the data they are processing in line with this guidance. If there is any data being processed that is not shown in these tables, staff must inform the Data Protection Officer so that it can be included.

8.3. As there is no national guidance on data retention periods provided by Ministry Division, the Ministry and Leadership team have produced their own policy.

Categories of data subjects covered by this policy are:

i. Ordination Candidates
ii. Reader Candidates
iii. Curates
iv. Clergy (CMD)
v. Clergy (MDR)
vi. BCDM / Lay Training

9. Procedure for dealing with CDBF Leavers IT Accounts

9.1. When a member of staff resigns, it is the line manager's responsibility to ensure that all of their staff member's files, documents and emails are audited prior to them leaving.

9.2. Any files, documents and emails that are no longer required must be permanently deleted.

9.3. Any files, documents and emails that are still required should be copied, named and stored in a designated Common File.

9.4. If any of these files contain personal data then they must not be accessible to anyone other than those who have a legitimate interest or consent to process the data.

9.5. On the day a member staff leaves:

i. HR will advise the IT of the name of the leaver
ii. HR will obtain the member of staff's computer password and email it to the leavers line manager.
iii. HR will advise the leavers line manager that the account will remain live for 6 weeks and then it will be permanently deleted.
iv. IT will be the line manager's responsibility to move any documents and emails that are required to a safe place during this period. They should also advise any of the leavers regular email contacts of who they should contact instead.
v. IT will disable remote access.
vi. IT will remove the leaver's entry from the global address book.
vii. IT will remove the leavers email address from any share address lists.

9.6. Six weeks after the leave date:

i. HR will advise the leavers line manager that the account will be permanently deleted the following day.
ii. HR will advise IT that the account can be deleted.
iii. IT will permanently delete the account the following day.

10. Policy review

10.1. This policy will be updated as necessary to ensure compliance with any changes or amendments made to legislation.

10.2. In case of any queries or questions in relation to this policy please contact the Data Protection Officer whose details are as follows:

Stephen Davenport
Director of Operations
Stephen.davenport@coventry.anglican.org
02476 521346

10.3. This policy will be reviewed at intervals of 2 years to ensure it remains up to date and compliant with the law.

Stephen Davenport

3 July 2025

Appendix 1

CiPD Guidance

The checklist below is divided into two parts:

- Records where there are statutory retention periods, with the statutory authorities.
- Records where there are no statutory retention periods, with recommended retention periods.

Statutory Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. If employers are in doubt, it's a good idea to keep records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.

Record types

Accident books, accident records/reports

Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).

Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records

Statutory retention period: 3 years for private companies, 6 years for public limited companies.

Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

Income tax and NI returns, income tax records and correspondence with HMRC

Statutory retention period: not less than 3 years after the end of the financial year to which they relate.

Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

National minimum wage records

Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover.

Statutory authority: National Minimum Wage Act 1998.

Payroll wage/salary records (also overtime, bonuses, expenses)

Statutory retention period: 6 years from the end of the tax year to which they relate.

Statutory authority: Taxes Management Act 1970.

Records relating to children and young adults

Statutory retention period: until the child/young adult reaches the age of 21.

Statutory authority: Limitation Act 1980.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity

Statutory retention period: 6 years from the end of the scheme year in which the event took place.

Statutory authority: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence

Statutory retention period: 3 years after the end of the tax year in which the maternity period ends.

Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

Working time records

Statutory retention period: 2 years from date on which they were made.

Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

Recommended (non-statutory) Retention Periods

For many types of HR records, there is no definitive retention period: it is up to the employer to decide how long to keep them. Different organisations make widely differing decisions about the retention periods to adopt. Employers must consider what a necessary retention period is for them, depending on the type of record.

The advice in this factsheet is based on the time limits for potential UK tribunal or civil claims. The period is often a question of judgement rather than there being any definitive right answer. For example, some records managers in public sector organisations recommend keeping an employee's records until they reach the age of 100, especially for pension purposes.

Employers should always review the length of time personal data is kept, consider the purposes of information when deciding how long to retain it, and update, archive or securely delete information if it goes out of date.

The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings. So where documents may be relevant to a contractual claim, it's recommended that these are kept for at least a corresponding 6-year period.

Record types

Actuarial valuation reports

Recommended retention period: permanently.

Assessments under health and safety regulations and records of consultations with safety representatives and committees

Recommended retention period: permanently.

Inland Revenue/HMRC approvals

Recommended retention period: permanently.

Money purchase details

Recommended retention period: 6 years after transfer or value taken.

Parental leave

Recommended retention period: 18 years from the birth of the child.

Pension records

Recommended retention period: until the employee reaches age 100.

Pension scheme investment policies

Recommended retention period: 12 years from the ending of any benefit payable under the policy.

Personnel files and training records (including formal disciplinary records and working time records)

Recommended retention period: 6 years after employment ceases.

Recruitment application forms and interview notes (for unsuccessful candidates)

Recommended retention period: 6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.

Redundancy details, calculations of payments, refunds, notification to the Secretary of State

Recommended retention period: 6 years from the date of redundancy

Senior executives' records (that is, those on a senior management team or their equivalents)

Recommended retention period: permanently for historical purposes.

Statutory Sick Pay records, calculations, certificates, self-certificates

Recommended retention period: The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there is a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.

Terms and conditions

Recommended retention period: review 6 years after employment ceases or the terms are superseded.

Termination of employment, for example early retirement, severance or death in service

Recommended retention period: at least 6 years although the ICO’s retention schedule suggests until employee reaches age 100.

Time cards

Recommended retention period: 2 years after audit.

Trade union agreements

Recommended retention period: 10 years after ceasing to be effective.

Trust deeds and rules

Recommended retention period: permanently.

Trustees' minute books

Recommended retention period: permanently.

Works council minutes

Recommended retention period: permanently.