

1 It is Synod Policy to comply with the requirements of the Data Protection Act, which has been extended and now covers the keeping of all records both electronically and on paper.

2 Under the new legislation, the ruling of the past few years that `local congregations of the United Reformed Church storing information on computer or disk and who are members of a Provincial (Synod) Trust need not register with the Data Protection Registrar (now called the Information Commissioner) providing that the Provincial (Synod) Trust has registered' **NO LONGER APPLIES.** However for most local churches the observance of principles of fair practice will mean that there will be no **need to register individually.** To comply with the Data Protection Legislation the following principles must be met and these apply to all those holding data **in any form whatever.**

All processing of personal data must be fair and should meet the following conditions:

- the person concerned (the data subject) has given consent - or is being used;
- to carry out a contract to which that person subject is a party;
- to meet a legal obligation of the data controller (i.e. the person responsible for the keeping of the record);
- to protect the vital interests of the person concerned;
- for various judicial and government functions;
- in the legitimate interest of date controller (unless it causes harm to the rights, freedom or legitimate interests of the person concerned).

Personal data can only be collected and used for specified purpose(s):

- the data must be adequate, relevant and not excessive;
- the data must be accurate and up to date;
- the data must not be held longer than necessary;
- the data subject's rights must be respected;
- you must have appropriate security.

Please note – special rules apply to the transfer of data abroad and are not dealt with in this note of guidance.

### 3 **What to do to ensure your church complies with the legislation**

#### **Draw up a policy**

This policy statement should cover such items as:

- why the information is to be held including any secondary use that will be made of it;
- what kind of information is to be held;
- whether any information is being collected without the knowledge of the person concerned;
- what types of disclosure that are likely to be made;
- how you intend to ensure that the information held is accurate;
- how long will need to keep the information;
- what level of confidentiality will be applied;
- any special security measures that apply.

#### 4 **Ensure those who have access to the data know exactly what they are allowed to do with people's information**

#### 5 **Ensure anyone about whom you hold information knows it is held, what it is used for and to whom you might pass it on.**

#### 6 **Get consent wherever possible for holding people's information and obtain explicit consent in writing if any detail could be classified as sensitive. The definition of `Sensitive information' includes racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sex-life or criminal record.**

**7 Make sure people are offered the chance to opt out of receiving any direct mailing, including fund raising. Design or modify your system so anyone may have access to their own record without being able to view others records. Make appropriate security arrangements for both manual and computer systems – as a minimum these should include passwords for computer systems and secure storage for manual records. Archive or delete records regularly.**

**8 A brief guide for those handling personal data:**

- when you hold personal data remember;
- it can only be used for the purposes for which it was originally obtained;
- you have to take good care of it;
- you have to use it fairly;
- you must ensure that it is adequate, relevant, not excessive, accurate, up to date and not being held longer than necessary;
- you are committing an offence if you get access to personal data you are not authorised to see, or if you disclose such data to other people;
- you are committing an offence if you sell personal data you are not entitled to.

**9 When you obtain personal data remember:**

- you must not deceive or mislead anyone;
- you must ensure the person concerned knows you are collecting the data and why and how it may be used;
- if data is provided from someone other than the individual concerned (the DATA SUBJECT) you must ensure the Data Subject knows you are using their data and why and how it will be used;
- you may have to get consent from the Data Subject to use their data, particularly if it is in any of the sensitive areas of racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sex-life or criminal record.

**10 When you disclose personal data remember:**

- you must check that the disclosure fits the purpose(s) for which the data is being held;
- you must check that the person you are disclosing it to is authorised to have it;
- you must check that the Data Subject is aware that this type of disclosure is possible or that there is an overriding reason, such as a legal obligation;
- if you put personal data on the WEB you will need consent from the data subject.

**11 Data subjects have rights too:**

- data can only be used if consent is given- but you can explain the consequences of withholding it;
- data cannot be used for direct mailing of any goods or services if the person concerned has refused permission;
- if you are telephoning people at home for direct marketing purposes you must check the number you are calling is not on a barred number register;
- data subjects can ask to see ALL the personal data you hold on them, including manual files.

**12 The Legal and Trust Officer holds a Data Protection Handbook at the Synod Office, entitled, **A complete guide to notification. The document** includes the following sections:**

- The notification life cycle;
- Completing the notification form;
- The Part 2 the Form;
- Completing the form on the internet;
- Notification exemptions;

- Changes introduced by notification;
- Glossary of terms.

The information contained in this guideline has been extracted from the URC Communications and Editorial Committee' booklet – The Data Protection Act and the Handbook mentioned above.

## **THE ARCHIVING OF CHURCH AND SYNOD RECORDS**

### **General**

- 1 The current information in the Synod Guidelines regarding the processing of data in accordance with the Data Protection Act 1998 (DPA) deals with the general handling of personal and sensitive personal data. You should refer to those guidelines for general information in relation to the application of the DPA. It is recommended that you remind yourself of those guidelines before reading these.
  - 1.1 These guidelines highlight issues to be addressed when archiving both automated and paper records from local churches and synods with a County Record Office (CRO) or a public library (PL), generally, upon closure and/or where the fellowship disperses, so as to comply with the requirements of the DPA.
  - 1.2 In January 2007, the URC History Society drew to the attention of Synods and local churches the need to preserve records for historical purposes. Such information is important for research, but can also be very helpful e.g. in resolving disputes over property, understanding past decisions made and remits of committees particularly if there are financial ramifications.
  - 1.3 Once a decision has been made to deposit material at a CRO or PL the data must be thoroughly scrutinised and any sensitive material should be marked "restricted access". This is a common practice and assists a CRO or PL in identifying personal or sensitive personal data. This is important as there should be no disclosure of "personal" data by them without having consulted the CRO or PL first and received specific instructions as to whether access to the data should be provided or not.
  - 1.4 All materials deposited with a CRO or PL will remain in the ownership of the local church/Synod and will be on permanent loan to the CRO or PL. This relationship should be clearly stated within the written agreement entered into between the local church and Synod and the CRO or PL before any deposit of records is made.
  - 1.5 As the material deposited is "permanently on loan" the local church/Synod will remain the data controller and therefore responsible for managing the observance of the requirements of the DPA including the eight data principles and the process by which access to personal and sensitive personal data is managed. The CRO or PL being the data processor should refer all requests for access to personal/sensitive personal data to the local church/Synod as the data controller to consider so that a decision can be made and instructions given regarding access. In view of this it is essential to have in place:
    - i A system to scrutinise all records before they are deposited (this will help to ensure that local churches and Synods are protected against an unauthorised disclosure of personal data within the records).
    - ii Ensure there is a paper trail available which demonstrates that all relevant issues have been considered in the scrutinising/decision-making process with regard to restriction and access.

**Steps to take following a decision to deposit data with a CRO or PL but before any actual deposit of records takes place:**

- i Following a process of due diligence to establish the suitability of the CRO/PL to receive and manage material, there should be a comprehensive written agreement between the local church and/Synod and the CRO/PL which regulates the deposit/security of and access to records and the relationship between them.
- ii A risk assessment should have been carried out in respect of the local church/Synod procedures regarding the process of scrutinising records and in respect of the depositing “process” in general.

**4 Risk Assessment in respect of local church/Synod procedures**

This should consider issues such as:

- i Is the process fully understood by those involved with it?
- ii Can the records to be deposited be identified?
- iii The criteria to be applied in making decisions to “restrict access” to personal/sensitive personal data;
- iv Is the procedure for scrutinising records up to date and is there a need for a review?
- v Is there a need to provide training or refresh training for those involved?
- vi The accuracy and completeness of material to be deposited;
- vii The security of the material to be deposited;
- viii Is the written agreement between the local church/Synod and the CRO or PL sufficient and up to date?
- ix Are procedures for considering the request for access to material and the providing of instructions to the CRO/PL sufficient?

**Do the procedures to be applied in relation to the data comply with the Data Protection Principles?**

Local churches and the Synod are reminded that they as data controllers should ensure that all personal/sensitive personal data is processed in accordance with the eight Data Protection Principles which are summarise as follows:

- i to process fairly and lawfully;
- ii to obtain personal data only for the purposes specified;
- iii to ensure that the data is sufficient for stated purposes relevant and not excessive;
- iv to ensure that the data is accurate and kept up to date where necessary;
- v to to keep the data any longer than necessary;
- vi to process the data in accordance with the data subject’s rights;

- vii to take appropriate technical and organisational measures against unauthorised processing of the data, its loss or damage to it;
- viii not to transfer personal data outside the European Economic Area without ensuring appropriate protection for the rights of the data subject (further advice should be sought should any such transfer be considered).

**Considering/identifying personal/sensitive personal data with material to be deposited:**

It is important that there is a clear and consistent procedure in place and that this is in writing... In general **personal data** is that which is:

- i biographical in a significant sense;
- ii the individual must be the focus of the information.

In general **sensitive personal data** is that which is personal data (as above) but also contains details of an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health or condition;
- sex life;
- alleged or actual criminal activity and criminal record

**When scrutinising records for 'personal' data consider whether**

- i The data is to be deposited in its entirety without restriction.
- ii The data is to be marked "restricted access".
- iii The 'personal data' is to be retained in its entirety and not deposited.

**It is recommended that all personal information should either be removed or marked "restricted access" so as to avoid the potential for unlawful disclosure, although the particular issue must remain a matter for local churches and the Synod to determine.**

**The counter argument to the above is that almost nothing is permanently sensitive; what is sensitive now will not be so in 50 or a 100 years' time. There is a danger of setting up a process which seeks to protect the present day and denies those in future years access to evidence which might be crucial to research about our social history, and the life of the church and fellowship some 50 or more years ago.**

**5 The process of due diligence in respect of a CRO/PL**

Before data is deposited with the CRO and/or PL it is important that a procedure of due diligence is conducted in order to establish that the body concerned is appropriate to hold the data. Issues to consider are e.g.

- i Competence of staff that will manage the deposited data, request for access, the application of the DPA and adherence to the terms of the written agreement with the Synod/local church.
- ii Does the body have procedures which comply in general with the seventh data principle regarding security and processing i.e. to take appropriate, technical and organisational measures against processing, or loss of, or damage to personal data:

Procedures to ensure the security of the data e.g. if any of the data is to be placed “on line” how will this be managed and who will have access to it (see schedule 1 for further guidance)?

#### 6 **The written agreement between Church and CRO and/or PL**

In order to comply with the seventh data principle to ensure that appropriate technical and/or organisational measures are taken against unauthorised/unlawful processing of personal data and against accidental loss or destruction or damage to personal data, then before data is deposited there **must** be in place a written agreement which regulates the relationship (see schedule 2 in this document at pages 7 and 8 for a guide list of issues that should be considered).

#### **Reminder**

#### 7 **Before a local church or Synod deposits any material with a CRO or a PL the following action must be taken:**

- the material to be deposited must be scrutinised by a competent person (usually the church secretary or appointed officer in Synod) and it is recommended any ‘personal’ data identified, packaged separately and marked “restricted access”;
- compile a list of all the material to be deposited. The original to be sent with the documents and a copy to be retained by the local church and a further copy sent to the Synod office for future reference;
- the written Agreement between the church and the CRO or the PL to be completed and signed, copied and the copy to be retained by the local church and sent to the Synod office for future reference.

In general the Agreement should deal with the following matters:

- |           |               |
|-----------|---------------|
| Section 1 | deposit;      |
| 2         | preservation; |
| 3         | conservation; |
| 4         | cataloguing;  |
| 5         | access;       |
| 6         | withdrawal;   |
| 7         | gifts.        |

#### **After deposit**

The CRO or the PL (also see Schedule 2) should send a letter of receipt with a schedule that describes the documents, shows an Accession number, a Catalogue Reference number, and will make reference to any restrictions on access to the records which should have been agreed. It is important to check that the details of restrictions are correct.

#### **Further information**

You are referred to the “Information Commissioners” website which has a considerable amount of information and guidance.

There is also a telephone helpline if required.

**SCHEDULE 1****DUE DILIGENCE**

Issues to consider before deciding if a CRO or PL is a suitable body with which to deposit records.

The following points are not intended to be exhaustive but an example of the kind of issues to consider.

The primary concern is observation of the seventh data principle with regard to the general security of data. Consider such issues as:

- i) Are there appropriate policies, risk assessments in place with regard to the holding, managing and security of data?
- ii) Is there adequate insurance cover in place?
- iii) Are there any conflicts of interest which could lead to breaches of confidentiality?
- iv) Are regular reviews of procedures carried out?
- v) Are staff that will come into contact with the data properly trained and conversant with the DPA? Are they trained on a regular basis?
- vi) What general security measures are there at the premises?
- vii) Are records held for other organisations? What are their experiences?

**SCHEDULE 2****Written agreements with a CRO/PL**

It is important that the written agreement sets out details of who it is between and the specifics of the relationship between the parties. Each agreement is likely to be particular to the circumstances that exist between the parties. Issues to consider are:

- i) the manner in which deposited material is to be processed and the process to be followed should a request for access be received;
- ii) confirmation that standards will be maintained regarding the quality of staff that will process data in terms of training in respect of the DPA and generally;
- iii) who it is that will be processing the data?
- iv) can the agreement be amended so as to comply with future requirements with regard to the processing of data and changes in law?
- v) the security of the data by appropriate technical, organisation/security measures;
- vi) the obligation to obtain and maintain appropriate insurance cover;
- vii) rights/obligations in respect of claims/indemnities regarding inappropriate processing of data and or damage to it;
- viii) the rights to access to data deposited by the local church/Synod.
- ix) distinguish such material as is deposited by way of gift and such as is to be held on permanent loan.
- x) the duration of the agreement/break clauses/review;
- xi) any charges that may apply/review of changes;
- xii) that the relationship will be regulated by the Laws of England and Wales;
- xiii) should disputes arise, how are these to be resolved e.g. arbitration or alternative dispute resolution, etc?

This list is intended as an illustration of the kind of issues to be considered and should not be viewed as being exhaustive.

## Records Advice for Churches

### 1 Introduction

#### **a. What this document covers**

This document gives guidance and advice on how URC churches should care for their paper and electronic records. It includes information on how long records should be kept for, how records should be managed and stored, what archives are and where they should be deposited.

#### **b. The importance of caring for your church's records**

Churches have a duty to care for their records; they are a valuable resource.

*Some of the reasons why a church should care for its records include:*

- Without proper organisation the sheer volume of records (paper and electronic) can become overwhelming. Well managed records ensure that the right information is available to the right people at the right time.
- Many areas of church activity are subject to external regulation, for example, child protection and finance, which makes it essential to maintain proper records.
- Good record keeping increases the church's accountability to its members, the synod, the URC and the wider community.
- It ensures that records that will have archival or historical value in future, and which help tell the story of the church, are identified and preserved.

### 2. Records retention - how long to keep records

Records must be kept for as long as they are required for operational, legal, historical etc purposes. However, it is also important that records that are no longer required are destroyed, for example, to prevent a build-up of obsolete records taking up valuable storage space.

The records retention schedule<sup>1</sup> in appendix 1 sets how long different types of church records should be kept for to meet business, fiscal, statutory etc requirements and when they can be disposed of. It also documents which church records should be offered to the local public record office to be kept as the church's archive.

### 3. Keeping records

#### **a. Paper records**

Paper records should be stored on church premises rather than in private homes. They should be kept in boxes or filing cabinets. The storage area should be as fire proof as possible; free from damp and mould; well ventilated; and unlikely to be affected by flooding, insect or rodent activity. Therefore, attics, basements, garages and outhouses are not suitable. All records should be kept where they are safeguarded against unauthorised access. Confidential, sensitive or important records should be stored in locked filing cabinets or safes and must be disposed of in a secure manner e.g. through shredding.

#### **b. Electronic records**

##### *Introduction*

Whilst information technology has made church administration much easier in many ways, there are certain challenges which are specific to electronic records and which must be considered.

##### *Long-term preservation and access*

Electronic records present particular challenges in terms of long-term preservation and access. Paper records can go decades before needing preservation work; long-term data preservation must be considered at the birth of each electronic record due to the relative instability of electronic media.

---

<sup>1</sup> A records retention schedule is a list of how long different sorts of records should be kept, and what to do with them after that time.

For example, software and hardware can quickly become obsolete due to rapid developments in technology; magnetic media is easily corrupted and data is not always retrievable; and data can be lost when migrating records to a new computer system.

As a result, guaranteeing long-term access to electronic records is difficult and requires more management, expertise and cost than guaranteeing long-term access to paper records. For this reason, it is recommended that any church records that need to be kept for longer than ten years or that have been designated as archives be printed and kept as paper records.

#### *Storage*

There should be a regular system of backup for electronic records saved on individual computers as a precaution against loss in the case of a hard drive failing, theft etc. These backups should be stored away from the computer, ideally in another building. Records stored on portable media such as CDs or USB flash drives should be checked regularly to ensure that they are still accessible.

#### *Management*

Electronic records should be managed in the same way as paper records. They should be saved into an organised filing system and subject to retention and disposal. It is important that electronic records are given titles that are understandable, describe what the record is and include its creation date. The record's title and date should be recorded within the document (for example, as a header or footer) so that they can still be identified when printed. As electronic records are easily altered it is helpful to identify different versions of a document by including version numbers or 'draft', 'copy' etc in the title and in the document itself.

#### *Email*

Emails are also electronic records and need to be managed. Unmanaged emails can be a source of stress for staff due to the large volume that they send and receive. Emails should be subject to the retention schedule. Transitory emails such as out-of-office replies should be deleted immediately; emails with short-term value such as notices of upcoming meetings should be kept in folders under the inbox and deleted when obsolete; records of value to the church should be saved into the folder system alongside other electronic records and the email deleted from the inbox; emails which have archival value or which need to be kept for more than ten years should be printed.

### **Archives**

4. **Archives** are the small percentage of a church's records that are preserved indefinitely because of their continuing value for legal, historical and research purposes.<sup>2</sup>

#### **a. 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.

#### **b. Archive deposit agreements**

It is helpful, before a deposit is made, to be clear on the terms of the transfer and to have a written contract between the church and record office setting out these terms. Things to be considered include:

- **When to transfer records:** records can be transferred to record offices when they are no longer required for current work purposes. The national URC records are transferred to the archive once they have reached 15 years old unless they are still required for operational purposes.

---

<sup>2</sup> An archive is also the building where archives are kept and the organisation responsible for the selection, care and use of records of continuing value.

Rather than making deposits of records sporadically it can be a good idea to make periodic transfers e.g. every five or ten years.

- **Loan/ gift:** are the records being given as a gift (transferring ownership) or a loan (retaining ownership)?
- **Access to the records:** Once records are transferred they will be made available to researchers according to the record office's access policy. It is important to ask whether the record office will accept records which the church wishes to keep closed to researchers for a fixed period of time. If the record office is not happy to accept these records, the church should consider keeping them until they are happy for them to be accessed by researchers.
- **Data Protection:** When arranging to deposit records, the church should talk to the record office about their policies on data protection. The record office will be able to offer advice, reassurance and information on how they manage records containing personal data.

#### c. **Preservation**

Any records that have been designed as archives must be printed and kept as paper records (although a digital copy may also be kept) as churches and most public record offices do not currently have the facilities for the safe long-term management of electronic records.

*For archival records, some simple preservation measures should be taken:*

- Brass or plastic paperclips should be used rather than metal paper clips, pins and staples which corrode and cause damage to documents.
- Avoid using staples and do not put papers into plastic pockets as these will have to be removed by an archivist before entering the archive.
- Do not use rubber bands on documents as these perish and cause damage to paper.
- Great care should be taken if storing documents in plastic wallets/ folders as certain types of plastic stick to the ink and lift it off the document.

#### d. **Archiving the church's website**

The UK Web Archive (<http://www.webarchive.org.uk/ukwa/>) 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.

### 5. **Data protection**

All URC churches are subject to the 1998 Data Protection Act. The Act sets out eight Data Protection Principles which must be considered when handling any records containing personal data. Information on Data Protection can be found on the Information Commissioner's Office website: [http://www.ico.gov.uk/for\\_organisations/data\\_protection.aspx](http://www.ico.gov.uk/for_organisations/data_protection.aspx).

### 6. **Further information/ advice**

For assistance or advice on matters of records and archives management, please contact Helen Weller or Jenny Delves on the contact details below.

Helen Weller, Archivist  
(Mon,Wed-Fri mornings)  
Westminster College  
Madingley Road  
Cambridge CB3 0AA  
Phone: 01223741084  
Email: [hw374@cam.ac.uk](mailto:hw374@cam.ac.uk)

Jenny Delves, Records Manager (Mon-Wed)  
United Reformed Church House  
86 Tavistock Place  
London WC1H 9RT  
Phone: 02079162020  
Email: [recordsmanger@urc.org.uk](mailto:recordsmanger@urc.org.uk)

## Appendix 1: Records retention schedule

### Key to the retention schedule

Retention periods which based on legal/ regulatory requirements are marked “[requirement]”.

### Records to be sent to the public record office

The following are records that should be preserved on a permanent basis. When they are no longer required by the church for operational purposes they should be deposited in the local public record office.

Type of record	Notes
Meeting minutes, agendas and supporting papers for church meeting, elders’ meeting, church groups	
Publications and resources	Includes church histories and magazines, memoirs of minsters or church members
Records documenting church events	Reports, programmes, photos. Not including records documenting the organisation of the event e.g. RSVPs
Baptism, marriage and burial registers	Store in a secure location, ideally a safe
Lists of members, and/or adherents	These should be dated
Orders of service	
Photographs	Dated with people and events identified
Final annual accounts (preferably signed)	
Architectural drawings, photographs, and plans for church and hall	
List of tombs in graveyards and inside the church	Copy inscriptions where possible

## Other records

Type of record	How long to keep it for	What to do with it
<b>General correspondence, enquiries etc</b>	Last action on correspondence + 2 years	Destroy
<b>Databases, mailing and contact lists</b>	Keep most up-to-date version	Destroy when no longer required
<b>Finance records</b> including: cash books, bills, bank statements, budgets, accounting records and other subsidiary financial records	Current financial year + 6 years [requirement]	Destroy
<b>Receiving and administering legacies, covenant payments and trusts</b>	Life of legacy/ covenant/ trust + 6 years	Destroy
<b>Records documenting the acquisition of ownership of properties</b>	Disposal of property + 12 years [requirement]	Destroy
<b>Records documenting the disposal of properties by sale, transfer or donation</b>	Disposal of property + 12 years [requirement]	Destroy
<b>Records documenting leasing-out arrangements for properties</b>	Expiry of lease + 12 years [requirement]	Destroy
<b>Deeds of title for properties</b>	Disposal of property	Transfer to new owner
<b>Records documenting applications for planning consents and consents granted</b>	Disposal of property OR Expiry of consent (whichever is sooner)	Transfer to new owner OR Destroy
<b>Records documenting major maintenance and development works on property</b>	Completion of work + 15 years OR Disposal of property [requirement]	Destroy OR Transfer to new owner
<b>Records documenting the negotiation, establishment, review and alteration of contracts and agreements between the church and others</b>	End of contract + 6 years [requirement]	Destroy
<b>Records documenting the arrangement and renewal of insurance policies</b>	Expiry of insurance policy + 6 years [requirement]	Destroy
<b>A note on the whereabouts of the Trust Deed(s), and any related documents, of the congregation<sup>3</sup></b>	Keep permanently	Keep permanently
<b>The Trust Deed(s), and any related documents, of the congregation</b>	Keep permanently	Keep permanently in a safe
<b>CRB disclosures<sup>4</sup></b>	Six months maximum [requirement]	Destroy
<b>Records relating to concerns about those working with children and young people</b>	Date of concern + 50 years	Destroy
<b>Allegation of a child protection nature</b>	Date of allegation + 50 years	Destroy

<sup>3</sup> If the Synod Trust is the trustee of the church building, ascertain whether these documents are held at the synod offices or with their solicitors. Congregations whose property is not held under the Synod Trust should inform the synod of the names of the trustees of the church buildings.

<sup>4</sup> The actual disclosure form must be destroyed after 6 months. However a record can be kept of the date of issue of a Certificate, the name of the subject, the type of Certificate requested, the position for which the Certificate was requested, the unique reference number and the details of the recruitment decision taken. A record of whether a disclosure was clear/ unclear or blemished **must not be kept**.

<b>against a member of staff/ volunteer, including where the allegation is unfounded</b>		
<b>Records of children's activities and events</b> e.g. registers, risk assessments; consent forms; insurance, health & safety records, incidents and application records; medical information; volunteers; accommodation lists	Date of activity/ event + 25 years [requirement]	Destroy
<b>Personnel records including:</b> contracts, appraisal records, job descriptions, training records, sickness records, termination of employment documentation	Termination of employment + 10 years [requirement]	Destroy
<b>Accident report</b>	Adult: date of incident + 3 years Child: until child reaches 21	Destroy
<b>An index to any church library</b>	Keep permanently	Keep permanently <sup>5</sup>
<b>A record of furnishings, lighting fixtures etc (with dates); artefacts given to church (include dates and origins); church silver, plate, china, mugs etc (with photographs in case of theft); memorial tablets (with a note of the text); war memorials (including note of text); stained glass.</b>	Keep permanently	Keep permanently

### Objects and memorabilia

Most churches will have collections of objects and memorabilia such as church silver, badges and banners from uniformed organisations etc which they will wish to keep. These items are not normally held by record offices. In the event of the closure of the church, the fate of such artefacts should be discussed with the synod and the record office who will be able to advise on a suitable home for them. Please note that items relating to Pilots companies can be given to the Pilots office in Church House.

<sup>5</sup> This should not be transferred to the archive in the event of the church closing.