



*The North Western Synod*  
*of the* **United Reformed Church**

# **General Data Protection Regulation**

**Guidance for  
Local Churches**



# Contents

Introduction	Page 4
Background Information	Page 5
Key Things for Elders to consider	Page 7
Establishing Good Data Protection Practice in your Church – Checklist	Page 10
Good Practice in Data Protection	Page 14
Further Information	Page 15

## Sample Forms & Templates

(These are also available separately from the North Western Synod Website)

Draft Privacy Notice	Page 16
Sample Consent Form	Page 19
Sample Consent Record	Page 20
Draft Retention Policy	Page 21
Example Data Audit Tool	Page 25



## Introduction

If a church holds personal data either on a computer or in a paper-based filing system it must follow the rules set out in the Data Protection Act 1998, and from 25th May 2018, the new General Data Protection Regulation 2016. This leaflet explains what this means for churches. It should however only be taken as general guidance and should not be used as a substitute for obtaining legal advice if necessary.

The leaflet includes a checklist for churches to work through. If churches have questions that fall outside the scope of this leaflet then we would advise that you contact the Information Commissioner's Office for their advice.

The General Data Protection Regulations came into force in May 2018. They update and extend the requirements on organisations of all sizes for the proper collection, use and storage of personal data. Local Churches need to be able to demonstrate that they have taken the appropriate steps to ensure that they comply with these requirements and that they are able to respond to any requests they receive about personal data. Compliance with the regulations is overseen by the Information Commissioner's Office (ICO) who have the power to ensure enforcement and in some cases issue fines for non-compliance.

The Elders (as the Trustees) of the local church are responsible for ensuring that their church has taken appropriate steps to comply with the regulations and to ensure that any issues regarding the personal data held by the church are dealt with in an appropriate manner.

This material is intended to provide Elder's with some initial guidance to ensure that they are able to meet these responsibilities and ensure that their church is able to comply with the regulations. It builds on the templates provided by the United Reformed Church nationally (available at <https://urc.org.uk/GDPR.html>) and provides more details about what Elder's need to do.

The leaflet also provides links to a number of church websites where more detailed information is available.

# Background Information

## What is GDPR?

The General Data Protection Regulation (GDPR) took effect in the UK in May 2018. It updated existing law on data protection (the Data Protection Act 1998). It provides individuals with more rights and protection in how their personal data is used by organisations. Local Churches must comply with its requirements, just like any other charity or organisation.

In the UK, compliance with data protection regulations is overseen by the Information Commissioner's Office (ICO). Most churches will be exempt from the requirement to register with the ICO, but a short online questionnaire is available on the ICO's website which will enable you to confirm this. The most likely reason why a church would need to register will be if it operates CCTV.

GDPR has made it more important that you are able to demonstrate that you have complied with the principles of good practice and regulations. This includes documenting your use of personal data and maintaining records that demonstrate this in practice, for example retaining records of consent given by people for the use of their personal data.

## Key Terms

There are a number of key terms which Elder's need to be aware of.

**Personal Data:** GDPR only applies to personal data. This is information relating to a living individual, who can be identified either directly from that data, or indirectly by combining this information with other data. This now includes internet / social media identifiers e.g. IP addresses, Facebook usernames etc.

**Special Category Data:** are specific types of personal data which the regulations consider to be particularly sensitive to the individual. This includes information about beliefs (including religion), health and well-being, race or ethnic origin.

**Data Processing:** means doing anything with personal data. It includes collecting the data, storing the data and sharing it with other people.

The **data subject** is the person about whose data is being processed.

The **data controller** is the person or group within the organisation who is responsible for deciding how personal data is processed in the organisation. In local churches this will normally be the Elders' meeting.

## **Principles of good practice**

### **Principles**

The regulations provide a framework of underlying principles that should guide the way in which we process personal data. These include:

- Data is only processed lawfully, fairly and transparently
- Data is only processed for specified purpose(s) and the data subject has been made aware of those purpose(s)
- Only data that is required for those purposes is collected and processed (i.e. the amount of data is minimised). Data is destroyed promptly once it is no longer required
- The data is kept accurately and up to date.
- Data is stored in a way which is safe and secure

### **Reasons for Processing**

There are a limited number of legal reasons why a local church can process personal data. Under GDPR, Churches must publish a privacy notice which sets out the reasons why you process personal information.

- Where it is necessary for legitimate interests of the church, for example to maintain a list of Members
- Where it forms part of a contract, for example where a church employs someone
- Where it is required for legal reasons, for example to respond to a safeguarding concern
- Where it is necessary in the legitimate interests of the individual, for example in a life and death situation
- With the explicit consent of the individual

### **Use of Consent**

It is important to recognise that GDPR has brought some significant changes to the use of consent as a reason for processing data. In particular:

- Consent must be explicit and affirmative (i.e. it involves a positive action). It cannot be assumed
- It can be revoked at any point in time and this must be actioned immediately

## **Rights of data subjects**

For a number of years, all data subjects have had a number of rights under the Data Protection legislation, GDPR has extended and strengthened these rights particularly where the data is held with consent.

The rights which will be most relevant to churches include:

- the right of access to a copy of their personal data (the right of subject access)
- the right to correct any mistakes in their personal information;
- the right to restrict or prevent their personal data being processed for direct marketing purposes (and in certain other limited circumstances);
- the right to erasure – subject to certain conditions e.g. if the processing of an individual's personal data is based upon their consent and after having withdrawn their consent for the processing, the church continues to hold the individual's personal data;
- the right to take proceedings through the civil courts against the data controller i.e. the Church Elders) for compensation where they have suffered serious damage or distress as a result of the processing of their personal information;
- the right to complain to the ICO if the data subject believes that the church has not handled their personal data in accordance with data protection law.

## **Subject Access Requests**

Any individual has the right to access the church to disclose to them all the information it holds about them. The information must be provided within 30 days of the request.

As well as the personal data held on your Church List, this request could include details of any emails or minutes of meetings which mention the individual person.

## **Data Breaches**

A data breach is the release of personal information to an unauthorised person (or entity). Although much of the media attention focuses on electronic information, data breaches are equally likely to occur through the release of paper based records.

If you discover a data breach you will need to assess the impact of the breach on the individuals whose data has been released. If the release could have a significant impact on an individual, you must notify them directly and potentially report the breach to the Information Commissioner's Office within 72 hours.

## Key Things for Elders to Consider

### 1. Who will be your data controller?

In most churches the data controller will be the Elders' Meeting. If this is the case, you need to agree that one of the serving Elders will act as the Church's Data Protection Lead.

### 2. Do we need to register with the Information Commissioner's Office?

Most churches will not need to register with the Information Commissioner's Office. There is a simple checklist available at <https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/> which you can use to confirm this. The most likely reason why you would need to register will be if you operate CCTV.

### 3. The Distinction between Church Members and other People

The regulations mean that you will need to think differently about the information you hold on Church Members and regular worshippers compared to other people

It is in the legitimate interests of the church to process personal information (contact details etc.) about people who are Members of the Church. The regulations provide

"that the processing is carried out as part of the legitimate activities of a non-profit body or association which exists for religious purposes and where the processing:

- is carried out with the appropriate safeguards for the rights and freedoms of data subjects
- relates only to individuals who are members of the body or who have regular contact with it in connection with its purposes; and
- does not involve disclosure of the sensitive personal data to a third party without the consent of the data subject.'

This does not cover special category data e.g. health information for which the consent of the subject will be required

For information about other people, for example friends and relatives of church members, other users of church premises etc. it is more likely that you will need their consent to process this information.

#### **4. The Use of Special Category Data**

Most churches will hold what is defined as special category data, e.g. information about people's health or personal circumstances. It will be unusual if this is not for clearly time-limited periods relating to a specific pastoral need.

The consent of the individual needs to be obtained and recorded. The Church Secretary (or Pastoral Care Secretary) should maintain a register of consent received for this type of information. A sample register is included in this leaflet.

Particular care needs to be taken about the circulation of this type of information. For example, information about people's physical or mental health often forms part of information circulated in prayer lists etc. This is sensitive (special category) data under the regulations and requires the explicit consent of the individual for processing, whether they are church members or not. It must be destroyed as soon as the purpose has expired.

#### **5. Taking Photographs and Videos**

Photographs of people form part of their personal information and the same regulations need to be followed if you are publishing photographs or videos where individuals can be clearly identifiable. This means you need the explicit consent for photographs of named individuals and for photographs including children under 16. It is good practice to ensure that there is an area in church where people who don't wish to be in any photographs or video recordings can sit outside the view of the camera.

#### **6. Websites**

Most websites collect data about visitors to the site through cookies. This is now more clearly included in Data Protection regulations and Elders' should check with your website provider what information is collected and ask them to provide a suitable website privacy notice to cover the processing of this information. The draft privacy notice contains an illustration of the wording that can be used.

#### **7. What do we need to do to comply?**

The URC has published a checklist, which sets out the steps that Elders' need to take to ensure that their church is meeting the requirements. An expanded version of this including some guidance notes is included in the next section of this leaflet.

Items 4 and 5 on the checklist about compiling a list of all the personal information held by the church is particularly important in ensuring that the church is able to demonstrate it is compliant and that it is able to respond to any requests from individuals about the information you are holding about them.

## Establishing Good Data Protection Practice in Your Church

REMEMBER - Data Protection legislation applies to both paper and electronic records and includes photos and videos as well as documents.

Tick when complete	Checklist	Additional Information
	<p>1. Confirm who is the Data Controller for your church. In most cases this is likely to be the eldership.</p>	<p>This needs to be clearly documented in the minutes of the Elders' Meeting. This means that all the Elders share a responsibility for the proper use of data by the Church. Most Churches will not need to register with the Information Commissioners Office, but there is a simple questionnaire on the ICO's website at <a href="https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/">https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/</a> which will enable you to confirm whether you should register.</p> <p>If you are appointing the Eldership as the Data Controller, it will be helpful if you appointed one of the serving Elders as the <b>Data Protection Lead</b> for the Church. They should report regularly to the Elders' Meeting on data protection compliance. As the Church Secretary is likely to be the main processor of data, good practice suggests that another Elder should take this role.</p>
	<p>2. Make sure that the Data Controller(s) understands what constitutes personal data. (Personal data relates to a <b>living</b> individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession.)</p>	<p>All Elders should understand the definition of personal data and the principles of good data processing set out in the current data protection legislation.</p> <p>A <b>separate guidance note</b> is available.</p> <p>It is important to remember that the definition is broad and includes things such as Photographs and Videos, social media accounts etc. as well as things that have traditionally been regarded as personal data.</p>

Tick when complete	Checklist	Additional Information
	<p>3. Make sure that the Data Controller(s) understand what constitutes SPECIAL CATEGORY (sensitive) personal data (i.e. data which contains information about: racial/ethnic origin; political opinions; religious or philosophical beliefs; TU membership; genetic/biometric for identification; health; sex life and sexual orientation. Special Category data can only be processed <b>with explicit consent</b>).</p>	<p>This category is particularly important for Churches as much of the data held by Churches could include data that falls into this category. For example, the category includes religious beliefs (e.g. church membership) and health information. There is an exception for information required to maintain membership records.</p> <p>However, this still means that most data that churches process will require the <b>explicit consent</b> of the data subject themselves. You need to record the consent and retain that securely in your records. You must remember that consent can be withdrawn at any point and you will need to ensure that any records you hold are updated immediately and old information destroyed.</p>
	<p>4. Compile a full list of <b>all</b> the types of personal data the Church collects and holds.</p>	<p>It will be helpful to have a formal document that records the information held by the Church. <b>A template and example is available.</b></p>
	<p>5. For each type of information determine where and how it is held.</p>	<p>This data schedule should include information about how the data is collected, recorded, processed, who it is shared with and how it is stored and for how long.</p>
	<p>6. Ensure that the data is held securely. Take steps to ensure that personal data is not disclosed to others without that person's permission – this includes: birthdays; addresses; telephone numbers; email addresses; matters relating a person's health.</p>	<p>This covers both electronic and paper records. Electronic records include emails and social media messages, so you must be particularly careful that distribution through these mediums is limited to those who have a right to receive this information, and that they understand that this information shouldn't be passed onto others without permission.</p>
	<p>7. For each type of information determine how long it should be held and be able to justify your decisions.</p>	<p>It will be helpful to maintain a simple data retention schedule which records how long your records are retained. <b>An example is available.</b> The schedule should be agreed by the Elder's Meeting and reviewed at regular intervals</p>
	<p>8. Dispose securely of any data which is no longer useful.</p>	<p>For paper copies of records this will normally mean that the copies should be shredded.</p>

Tick when complete	Checklist	Additional Information
	<p>9. For each type of information establish a routine for the permanent and secure disposal of time-expired data.</p>	<p>A logical time to do this will be immediately following your Annual Church Meeting, when it is likely that any changes to roles within the church have taken place. The regular routine needs to include:</p> <ul style="list-style-type: none"> <li>• Removing access to information from those who are no longer office holders</li> <li>• Enabling all members to update their information and consent</li> <li>• Disposing of all expired data</li> </ul>
	<p>10. Determine who will deal with Subject Access Requests (SAR). Usually the Church Secretary.</p>	<p>If you have appointed a Data Protection Lead, the responsibility for responding to these should rest with them.</p> <p>In most cases, it is unlikely that a church will have difficulty in meeting the 30 day deadline.</p>
	<p>11. Make sure that the Church Secretary or other relevant person(s) know that there is a statutory limit (30 days) within which to comply with a Subject Access Request.</p>	<p>It is important that the information is thoroughly checked before the response is sent, and for example you have ensured that the personal information relating to any other person is thoroughly redacted.</p>
	<p>12. Complete and publish your church's Privacy Statement.</p>	
	<p>13. Make sure that the Privacy Statement is posted in a prominent position and that members, friends and adherents are aware of its existence and that copies are available for them to take away.</p>	<p>If your church has a website the Privacy Policy can be simply published there. <b>A template is available</b> which includes your data retention schedule.</p> <p>If you are updating your records of consent, you can use the Privacy Statement to provide people with information about how you are going to use their information.</p>
	<p>14. Bring the Privacy Statement to the notice of members at a Church Meeting and review regularly its effectiveness - suggest at Annual Church Meeting.</p>	

Tick when complete	Checklist	Additional Information
	15. Monitor, review and amend as necessary.	The Elders' meeting should review the Privacy Statement and other aspect of your Church's approach to data protection on a regular basis, normally annually. The outcomes of the review should be recorded in the minutes of the meeting
	16. Ensure that the Church has clear procedures to respond to a data breach	The Elders' Meeting should ensure that they have agreed procedures to deal with a suspected data breach, and that this ensures that the requirements for example of notification to affected individuals are clearly understood
	17. Ensure that the Church website includes a privacy notice relating to the collection of cookies from visitors to the site	The Elders' Meeting should contact your Website provider / hosting organisation and seek information about the collection of cookies on the website and ask them to provide and appropriate website privacy notice about the processing of such data collected on the website

## **Good Practice in Data Protection**

This section provides some examples of good data protection practice.

### **Record Keeping**

Ensure that paper records e.g. Church Directories are kept securely both on Church Premises and by individual Elders/ church officers

Ensure personal data held on computers is properly protected by passwords or encryption

Ensure that the accuracy of information is checked regularly and promptly updated

As soon as the information is no longer required ensure that it is destroyed, e.g. old prayer lists

Ensure that former officers / elders return or destroy copies of church directories etc. and confirm that this has been done

### **Emails**

Ensure that circulations are done using the bcc facility. This prevents other individuals accessing people's email addresses

Don't use shared personal email addresses (e.g. Husband and Wife) to send personal information

Consider ensuring that the minister and church officers have church email addresses

### **Consent**

Ensure that the sharing of any personal information is supported by the consent of the individual. Examples include – including birthday greetings in the Church Newsletter, pastoral concerns in prayer lists

Don't disclose personal information (e.g. address, contact information etc.) to a third party without the individual's permission. Offer to pass the requester's contact information to the individual for them to make contact.

Don't assume that an individual's consent will last forever. Ensure that it is regularly updated and the record of consent retained

### **General**

Always remember that an individual has the right to see ALL the information you hold about them (or that refers to them), both facts and commentary, so ensure that all recorded information is accurate and you would be happy to share it with the individual

Don't assume that data breaches relate solely to computer hacking – it is as likely to result from the loss of paper records left unattended in a public place e.g. church porch or office.

Don't assume that data protection doesn't matter or it is someone else's responsibility – IT DOES and everyone has a part to play.

## **Further Information**

There are a number of useful sources of information for churches on the internet. Many of these also contain templates that you can use to help you with meeting the regulations.

Information Commissioner's Office      [www.ico.org.uk](http://www.ico.org.uk)

URC Material      <https://urc.org.uk/GDPR.html>

## **Other Churches**

Baptist Union

[https://www.baptist.org.uk/Groups/302154/Data\\_Protection\\_and.aspx](https://www.baptist.org.uk/Groups/302154/Data_Protection_and.aspx)

Church of England

<https://www.manchester.anglican.org/gdpr/>

<https://www.parishresources.org.uk/gdpr/>

Methodist Church

<https://www.t MCP.org.uk/about/data-protection>

## **Safeguarding Concerns**

Baptist Union guidance:

<https://www.baptist.org.uk/Publisher/File.aspx?ID=209333&view=browser>

# SAMPLE DATA PRIVACY NOTICE

## Local URC Church

### 1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

### 2. Who are we?

The **Elders' Meeting of Local URC Church** is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

### 3. How do we process your personal data?

The Elders' Meeting of Local URC Church complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To administer membership records;
- To fundraise and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at **Local URC Church**;
- To provide contact details of officers and others with specific responsibilities (egg DBS signatories) to the synod office and Church House. This enables the synod and national administration of the United Reformed Church.
- To share your contact details with the Synod office so they can keep you informed about news in the synod and events, activities and services that will be occurring in the area and in which you may be interested.

#### **4. What is the legal basis for processing your personal data?**

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and keep you informed about other church events.
- Processing is necessary for carrying out legal obligations in relation to Gift Aid or under employment, social security or social protection law, or a collective agreement;
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided: -
  - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
  - there is no disclosure to a third party without consent.

#### **5. Sharing your personal data**

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the church with your consent.

#### **6. How long do we keep your personal data?**

We keep data in accordance with the guidance set out in our data retention schedule which is available on our website.

Specifically, we retain contact information for 12 months after the last contact; gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and statutory registers (baptisms, marriages, funerals) permanently.

#### **7. Your rights and your personal data**

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the **Elders' Meeting of Local URC Church** holds about you;
- The right to request that the **Elders' Meeting of Local URC Church** corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the **Elders' Meeting of Local URC Church** to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where

applicable) *[Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means]*.

- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) *[Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics]*
- The right to lodge a complaint with the Information Commissioners Office.

## **8. Cookies on our website**

Our website includes “performance” cookies. These collect information about how visitors use a website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don’t collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how a website works. ‘Performance’ cookies stored when a user visits this website record Country, IP Address, Operating system and Browser type. These are shared with Google and Bing for analytical purposes

## **9. Further processing**

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

## **10. Contact Details**

To exercise all relevant rights, queries or complaints please in the first instance contact **Church Secretary** at **[insert contact details]**.

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

**Elders’ Meeting Local URC Church**

**Date**

## Local URC Church

### Sample Consent Form – Contact Information

Your privacy is important to us, and we want to communicate with church members and regular worshippers in a way which has their consent, and which is in line with UK law on data protection. As a result of a change in UK law, we now need your consent as to how we contact you. Please fill in the contact details you want us to use to communicate with you:

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Email Address: \_\_\_\_\_

Phone Number: \_\_\_\_\_

By signing this form you are confirming that you are consenting to the Elders of **Local URC Church** holding and processing your personal data for the following purposes (please tick the boxes where you grant consent) :-

I consent to the church contacting me by  post  phone or  email.

To keep me informed about news, events, activities and services at **Local URC Church** (note you can unsubscribe from the church e-bulletin at any time);

To including my contact information in the 'Church Directory' which is circulated to Church Elders and Office Holders.

To share my contact details with the United Reformed Church North Western Synod and Trust so they can keep me informed about news, events, activities and services that will be occurring in the Synod and which are directly relevant to the role I am undertaking;

Signed: \_\_\_\_\_ Dated: \_\_\_\_\_

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or to protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Church Secretary.

You can withdraw or change your consent at any time by contacting the Church Secretary at **Local URC Church Church Office, Church Road, Anytown AB1 2CD** or [secretary@localchurch.org.uk](mailto:secretary@localchurch.org.uk). Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

## Local URC Church

### Record of Consent for Sensitive Personal Information

<b>Who consented?</b>	<b>When did they consent (date / time of consent)?</b>	<b>What information did they consent to sharing and for what purpose?</b>	<b>How did they consent?</b>	<b>Has consent been withdrawn?</b>
<i>e.g. name of individual who gave consent</i>	<i>Date / time of conversation of email</i>	<b>Be specific about what information they agreed to share and for what purpose e.g. to include in prayer list, to update Elder's Meeting</b>	<i>Verbally or Writing</i>	<i>Only complete if consent is withdrawn and note date</i>
Mr Smith	06.05.18	Information about their current illness for inclusion in this week's prayer list	Verbally to Mrs Jones on pastoral visit	
Mrs Clark	11.05.18	To ask if Elders could be told that she was going to stay at her sister's for convalescence after hip operation	Email to Church Secretary	Yes on return 26.05.18

**URC North Western Synod: Illustrative Document Retention Schedule for Local Churches**

<b>Section</b>	<b>Documents</b>	<b>Retention period</b>	<b>Reason</b>	<b>Action after Retention Period</b>
<b>Membership</b>	Church Membership List (Names)	Indefinitely but reviewed and updated regularly	Good practice	To Archive if church closes
	Contact details of Church Members, adherents, and friends	12 months after individual has ceased to be a member or last made contact. <sup>(1)</sup>	Good practice	Destroy
	Church Contact list or Directory	1 year after publication	Good practice	Destroy
	Junior Church Roll	Until the child/young adult reaches the age of 21	Good practice	Destroy
<b>Statutory and other Registers</b>	Contact details for parents / guardians of Junior Church members	12 months after the individual has last made contact. <sup>(1)</sup>	Good practice	Destroy
	Register of Baptisms / Cradle Roll	Indefinitely	Statute	To Archive if church closes
	Registers of Marriages	As determined by the Registrar General	Statute	To Archive if church closes
	Register of Funerals	Indefinitely	Statute	To Archive if church closes
	Grave Records	Indefinitely	Statute	To Archive if church closes
	Church Meeting Minutes	10 years from the date of the meeting <sup>(2)</sup>	Good practice	Archive (e.g. County Archive Office)
<b>Meetings</b>	Trustee Meeting Minutes	10 years from the date of the meeting <sup>(2)</sup>	Good practice	Archive (e.g. County Archive Office)
	Minutes of internal groups	5 years from the date of the meeting	Good practice	Destroy unless of particular value in which case send to Archive

*(1) Unless individual asks for their details to be removed immediately*

*(2) These should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the church before sent to archives.*

<b>Section</b>	<b>Documents</b>	<b>Retention period</b>	<b>Reason</b>	<b>Action after Retention Period</b>
<b>Finance</b>	All financial records – invoices, bills, bank statements, paying in books etc.	6 years from the end of the financial year the record relates to	Charities Act and HMRC Rules	Destroy
	Payroll records including correspondence with HMRC	6 years from the end of the financial year the records relate to.	Charities Act and HMRC Rules	Destroy
	Gift Aid declarations and associated paperwork	6 years after the last receipt and claim	HMRC Rules	Destroy
	Legacy information (i.e. documents which relate to a legacy received by the church)	6 years after the deceased's estate has been wound up	In line with requirements for other financial information	Destroy
	Church Annual Accounts and Reports	10 years <sup>(2)</sup>	Good practice	Archive (e.g. County Archive Office)
	Leases	12 years after lease and liabilities under the lease have terminated	Limitation Act 1980	Destroy
<b>Property and Contracts (Property Deeds and Contracts will normally held by the NW Synod Trust rather than by the individual church)</b>	Records of Statutory Inspections e.g. Gas, Electrical, Portable Appliances	Until the next test or for the lifetime of portable equipment	HSE Guidance	Destroy
	Final plans, designs and drawings of the building, planning consents, building certifications, collateral warranties, records of major refurbishments and redevelopments.	Permanently or until six years after property is disposed of	Limitation Act 1980	Destroy 6 years after property is disposed of
	Insurance Records	Indefinitely	Impact of historic cases	To Archive if church closes

<b>Section</b>	<b>Documents</b>	<b>Retention period</b>	<b>Reason</b>	<b>Action after Retention Period</b>
<b>Employment</b>	All information relating to recruitment, selection and development whilst in post	6 years after post-holder has left your employment	Limitation Act 1980 <sup>(3)</sup>	Destroy
	Information on any disciplinary or grievance matter that is still 'live' on the individual's personnel file, including information on any penalty or warning imposed	6 years after post-holder has left your employment	Limitation Act 1980 <sup>(3)</sup>	Destroy
	Information on an individual's health and sickness record, including information on any adjustment made to their working pattern, either on a temporary or permanent basis	6 years after post-holder has left your employment	Limitation Act 1980 <sup>(3)</sup>	Destroy
	Parental leave records	18 years from the date of the birth of a child	To enable future employers to check entitlement	Destroy
	Pensions Records	According to the schedules set by the Pension provider		Destroy
	Application forms and interview notes for unsuccessful candidates	6 months to a year	2010 Equality Act recommends six months. One year limitation for defamation actions under Limitation Act.	Destroy

*(3) Six years is generally the time limit within which proceedings founded on contract may be brought*

<b>Section</b>	<b>Documents</b>	<b>Retention period</b>	<b>Reason</b>	<b>Action after Retention Period</b>
<b>Health and Safety</b>	Reportable accidents	3 years after date of accident or end of any investigation if later	H&S Regulations	Destroy
	Accident Books	3 years after the date of last entry	H&S Regulations	
	Records documenting external inspections	3 years after date of inspection	Good practice	Destroy
<b>General</b>	Correspondence (paper and emails)	Unless this relates to any other category of data listed here (e.g. finance, employment, safeguarding etc.) correspondence should be kept for as long as is relevant. Churches might find it helpful for staff and volunteers to have an annual 'purge' of all correspondence and destroy any which is no longer relevant.		
	Personal Data relating to Church events	Disposed of immediately after event unless anything has occurred (e.g. Accident, Safeguarding concerns) which indicates that records should be retained for a longer period.		
	Photographs and Videos of events	Only limited items should be retained for more than 2 years after the event for historic records; e.g. removed from website	Good practice	Destroy
<b>Safeguarding</b>	Information on any safeguarding concern involving employee, minister, volunteer	75 years after role / involvement in church ceases	Requirements of Independent Inquiry into Child Sexual Abuse (ICSA)	Destroy
	A comprehensive list of what is regarded as relevant safeguarding information in churches is found in the Baptist Union's document "Safeguarding Record Keeping" which can be accessed on <a href="https://www.baptist.org.uk/Publisher/File.aspx?ID=209333&amp;view=browser">https://www.baptist.org.uk/Publisher/File.aspx?ID=209333&amp;view=browser</a> . Relevant records can include records relating to Employment, Discipline, Events, DBS Clearances as well as specific allegations. For more information contact the Synod's Safeguarding Officer.			

## Local Church EXAMPLE Data Audit Tool

Description of the data	Whose data is being held?	Is this Special Category Data?	Why is the data held and what is it used for?	What is the basis for processing the data (e.g. legal obligation, consent etc.)	Who holds the data and who can access it?	What security controls are in place?	Is the data shared outside the church? If so who with?	How long is data kept for? What happens after that time?	Is this covered by our privacy notice?	What actions are required to ensure compliance?
Elders and Officers contact details	Serving Elders and Church Officers	No	To maintain register of church officers	Legal Obligation	Church Secretary (copies to all serving Elders)	Computer file on Secretary's PC and paper copies kept in filing cabinet	Yes with Synod	Updated annually and old copies destroyed	Yes	Password protect file and ensure security of paper copies
Gift Aid Declarations	Church Members and Regular givers	No	For claiming Gift Aid	Legal obligation	Held by Gift Aid Officer. Also accessed by treasurer	Paper declarations kept in a filing cabinet. Spreadsheet on PC.	Yes with HMRC	Six calendar years after last gift claimed on the declaration	Yes	Password protect the spreadsheet
Pastoral Concerns / Prayer List	Church Members and others	Yes	Information on health etc. of people known to the church	Consent (Special Category Data)	Pastoral Secretary / Minister	Computer file	No	Prayer list is destroyed immediately after service each week	Unsure	Password protection. Check Privacy notice for clarity
Birthday List for church newsletter	Church Members and others	No	To include list of birthdays in newsletter	Consent	Newsletter editor	Computer File	No	Data is deleted 18 months after last contact	Yes	Check password protection