The Bridges Group of Parishes

Lower Shuckburgh, Napton & Stockton, with Priors Marston, Priors Hardwick & Wormleighton

Data Protection Policy

Everything starts with God. He is personal. He created and sustains the world and remains actively involved in it, particularly in his son Jesus. The single quality of God that is predominant throughout scripture is His "steadfast" love. Another constant theme is safety. In our troubled world, God offers a haven, a safe space for the weak, the poor and the vulnerable. He is also passionate about justice: He gives a voice to the voiceless. These themes of love, protection and justice combine in the Fatherhood of God and are modelled by Jesus. We too must therefore ensure that love, safety and justice are embedded in our culture and ethos.

Introduction

The General Data Protection Regulation (GDPR) took effect in the UK on 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by organisations. It applies to any organisation that holds and processes personal information about people. PCCs and incumbents must comply with its requirements, just like any other charity or organisation. But it is important that anyone who handles data on behalf of the Bridges Group is also aware of how it applies to what they do.

Definitions

- *Personal data* is information relating to a living individual who can be identified directly from that data or indirectly by reference to other data held.
- *Processing* is anything done with/to personal data, including its retrieval, management, transmission, destruction and retention.
- The *data subject* is the person about whom personal data are processed.
- The *data controller* is the person or organisation who determines the how and what of data processing, in a parish that is usually the PCC or incumbent.

Underlying principles

The law requires that data:

- will be processed lawfully, fairly and transparently;
- is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent;
- collected on a data subject should be "adequate, relevant and limited." i.e. only the minimum amount of data should be kept for specific processing;
- must be "accurate and where necessary kept up to date";
- should not be stored for longer than is necessary
- storage is safe and secure in lockable filing cabinets or in password protected computer files. Unprotected data should not be left unattended.

Good practice

With the introduction of GDPR, it is vitally important that everyone understands the importance of data protection. All PCC members and other key data users should be made aware of the

requirements of the new law and receive basic information so that good decisions can be made to implement the GDPR.

The compilation of the data audit of all databases, email lists, spreadsheets, paper documents and other lists of personal data will identify:

- what personal data is being held
- the legal basis for holding it
- who holds the data
- who can access the data
- what security controls are in place
- whether consent has been obtained
- how long the data is kept
- any further action required to comply with GDPR and improve good practice

Privacy and data protection should be a core part of any new initiative and not merely an afterthought. It is important that those planning new initiatives consider data protection in the early planning stages to ensure a compliant solution. Any new processing operation will require a Data Protection Impact Assessment (DPIA). (See Appendix A)

Accountability

One of the main changes is that the GDPR places a much greater emphasis on transparency, openness and accountability i.e. documents must be kept in order to prove compliance with the legislation. Decisions and actions taken about processing activities, information distributed and reviews of policies and processes should be documented.

Data Protection Compliance Officer (DPCO)

A DPCO will be appointed to:

- inform and advise members and volunteers of the Bridges Group about their obligations to comply with the GDPR and other data protection laws;
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, raising awareness and circulating advice;
- advise on and monitor data protection impact assessments;
- act as the contact point for, and to cooperate with the ICO, and to consult on any data protection matters;
- be the contact point for individuals whose data is processed.

Legal bases for processing personal data

There are several legal bases for processing data. Those which apply directly to the Bridges Group are:

- **Legal obligation** (i.e. a legislative requirement, such as processing gift aid applications or processing data in relation to the electoral roll, in compliance with the Church Representation Rules);
- **Legitimate activity** as carried out by us as a not-for-profit religious body (e.g. general administration of church groups – where the information is shared with others in order to carry out a service to other church members);
- **Explicit consent** to keep members of the church informed about news, events, activities, services and initiatives (e.g. sending out a newsletter). (See Appendix B for the standard consent form.)

Consent
Consent is not an easy option under the GDPR so other legal bases should be considered as a first option.

Where we do rely on consent as the lawful basis for processing any personal data, for that to be valid under the GDPR, consent must be fully documented, freely given, specific, informed, unambiguous and able to be withdrawn at any time. We therefore need to take a view on what effect either the refusal or withdrawal of consent will have on our processing activity.

Where we require explicit consent, the wording must be sufficiently strong to allow us to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting and suffers no detriment by not providing consent. We must also tell individuals that they have the right to withdraw consent at any time and ensure that the procedure for withdrawing consent is just as simple as granting consent, (e.g. by sending an email or (un)ticking a box). Consent may be relatively straightforward to achieve where it is being sought for a single purpose, for instance, signing up to a newsletter but it will be potentially much more difficult to demonstrate that we have complied with all the conditions that constitute valid consent where the personal data is to be used for multiple purposes, as we will need to ensure that consent is valid in relation to each purpose.

We will need to keep records of all consents received and periodically review (e.g. every 5 years) them to ensure that they are still valid, and a separate list of refused or withdrawn consent, so we do not process the personal data of that person for that purpose.

Individuals' rights
The GDPR includes the following rights for individuals:

- **The right to be informed**
  Individuals continue to have a right to be given "fair processing information". This will usually be through a privacy notice (see Appendix C). When personal data is collected, the individual will be given certain information, such as our identity and how we intend to use their information. The privacy notice will be available on our website and from the Group Administrator and will be reviewed annually. It will also be included on any paper forms.

  Under the GDPR additional information will need to be supplied. This will include the lawful basis for processing their data; our data retention periods (how long we keep it for); who we will share it with and that individuals have a right to complain to the Information Commissioner's Office (ICO) if they think that there is a problem in the way that we deal with their personal data.

- **The right to access, including subject access requests (SAR)**
  Individuals have the right to be given confirmation that their data is being processed if they ask. This should be done using an SAR form (see Appendix D) The GDPR allows individuals to access their personal data so that they are aware of and can check the lawfulness of the use and the accuracy of the data. This information needs to be given in a permanent form.

  Initially this will be done by the DPCO who will verify the requestor's identity before proceeding to retrieve the information requested within the required timescales (normally one month) and

without disclosing other information in the process. A log will be kept of the request and each stage of the response process will be tracked and documented for audit purposes.
We will be able to refuse or charge a "reasonable fee" (based on the administrative cost of providing the information) for requests that are manifestly unfounded, excessive or repetitive. If we do refuse a request, we must tell the individual why and that he/she has the right to complain to the ICO or seek a judicial remedy.

- **The right to rectification (correction)**
  Individuals have the right to have their personal data rectified (corrected) if it is inaccurate or incomplete. If the data has already been given to third parties, we must tell those third parties of the correction. We must also tell the individuals about the third parties to whom the data has been given.

- **The right to erasure (also known as the right to be forgotten)**
  Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This means that although a person can request that his/her personal data be deleted immediately, if the purposes for which the data was collected still exist then unless it was given by consent and they are withdrawing their consent, we do not have to agree. For instance, safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and proportionate – e.g. to protect members of the public from significant harm. Another example is that some financial information, such as that relating to gift aid, cannot be deleted immediately due to financial auditing regulations. The personal data on the electoral roll can only be deleted in accordance with the Church Representation Rules. Examples include, if someone writes stating that they no longer wish to be included on the roll or a person no longer lives in the parish and no longer attends public worship there. Information in parish registers cannot be deleted under any circumstances. (See Appendix E for a summary of the requirements for the retention of records.)

- **The right to restrict processing**
  Individuals have the right to restrict processing of their personal data in certain circumstances. For instance they may consider the processing to be unlawful and rather than request erasure, they ask that it be restricted, i.e. that the processing is limited in some respect; or where there is a challenge as to its accuracy, we may need to restrict the processing until this is resolved. If processing is restricted, we can still store the data but cannot otherwise use it, and we should retain sufficient information to alert us to the restriction applied.

- **The right to data portability**
  This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT system to another. It only applies in certain circumstances and is highly unlikely to affect us.

- **The right to object**
  Individuals have the right to object to processing in certain circumstances – e.g. If we have relied on legitimate interest to process data and an individual is not happy with this they have the right to object to us processing their data.

- **The right not to be subject to automated decision-making including profiling**
  The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention.

Processing personal data about children
The GDPR brings into effect special protection for children's personal data, particularly in relation to online services, such as social networking. If we offer online services directly to children and rely on consent to collect their information, we will need a parent's or guardian's consent to lawfully use that data if the children are under the age of 13 (this is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).

We must also be able to show that we have been given consent lawfully and therefore, when collecting children's data, we must make sure that our privacy notice is written in a language that children can understand, and copies of consents must be kept.

Where we are processing children's personal data that is not part of an online service there are no specific additional requirements. The GDPR does state that specific protection is needed where children's personal data is used for marketing purposes or creating personality or user profiles. Ultimately, we must consider the need to protect children's personal data from the outset and design systems and processes with them in mind.

Personal data breach
The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

A *personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Personal data breaches may arise from a theft, an attack on our IT systems, the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure.

We should make sure that everyone understands what constitutes a personal data breach, and that this is more than a loss of personal data. An internal breach reporting procedure will be put in place to facilitate decision-making about whether we need to notify the ICO or affected individuals.

We have to notify the ICO of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of individuals i.e. if unaddressed such a breach is likely to have a significant detrimental effect on individuals (e.g. it will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage). This will be assessed on a case by case basis.

A breach notification to the ICO will contain:
- a description of the nature of the personal data breach including, where possible
  - the categories and approximate number of individuals concerned;
  - the categories and approximate number of personal data records concerned;
- a contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;

- a description of the measures we have taken, or proposed to take, to deal with the personal data breach and, where appropriate, the measures we have taken to mitigate any possible adverse effects.

A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay. It may not always be possible to investigate a breach fully within that time-period and so we can provide information in phases.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay. We need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures we have taken, or propose to take, to deal with the personal data breach and including, where appropriate, the measures we have taken to mitigate any possible adverse effects.

Even where a breach doesn't need to be reported, we must document the breach including the facts relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability principle, and allows verification of our organisation's compliance with our notification duties under the GDPR.

However a breach occurs it is important that we deal with it effectively and learn from it. We should have a Breach Register to record incidents and the process used to investigate and implement recovery plans. We should monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.

Information security

Security must be appropriate to the nature of the data held and the harm that may result from its improper use, accidental loss or destruction. Systems should be in place to minimise a potential personal data breach. Examples include:

- Technological
  - installation of a firewall and anti-virus software
  - systems to receive automatic updates
  - restrict authorisation to access data
  - restrict access via the use of strong passwords
  - restrict use of mobile equipment for accessing data (e.g. laptops, USB devices, smartphones)
  - have a robust data back-up strategy
- Emails – to avoid accidental disclosure or human error:
  - select the right address from a drop-down menu
  - use the "blind carbon copy" (bcc) function if there are multiple recipients
  - take extra care that entries are still valid when using group email addresses
  - recognise and do not respond to phishing emails
  - do not open spam
- Physical
  - check the security of paper files (e.g. locked filing cabinets)

- shred documents containing personal data
- check the physical security of premises

- Management and organisational measures to build a culture of security awareness:
  - appoint someone to act as DPCO
  - circulate regular advisory updates
  - review policies
  - audit processing activities

Data retention and disposal
See Appendix E for details of how long data will be held and how it will be disposed of.

Data sharing
All personal data will be treated as strictly confidential and will only be shared with other members of the Group in order to carry out a service to other members or for purposes connected with the Group. We will only share data with third parties outside of the Group with the express consent of the data subject and it has an appropriate lawful basis.

Further advice
Further advice is available from:

- The ICO publishes useful and up to date guidance and resources for data protection: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- The National Church Institutions GDPR Working Group can be contacted via gdpr@churchofengland.org
- There is a useful checklist and other resources online at: www.parishresources.org.uk/gdpr
- For legal advice we must contact the Diocesan Registrar whose details can be found from the Diocesan Office or from the Diocesan website

This policy was agreed across the Group and adopted 1st July 2018

Appendix A - Data Protection Impact Assessment – Not available yet
Appendix B – Standard consent form
Appendix C - Privacy notice
Appendix D - Subject Access Request (SAR) form
Appendix E - The retention of records

Appendix B

The Bridges Group of Parishes

Lower Shuckburgh, Napton & Stockton, with Priors Marston, Priors Hardwick & Wormleighton

Your privacy is important to us and we want to communicate with church members 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 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(s): ……

By signing this form you are confirming your consent to the Bridges Group of Parishes holding and processing your personal data to keep you informed about news, activities, events, services and initiatives across the Bridges Group of Parishes.

I consent to the Bridges Group contacting me by: ☐ post ☐ phone ☐ email.
(Tick all boxes as appropriate)

Signed: ……

Dated: ……

If 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 activities) except in certain limited situations, such as where we are 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 on our website (www.thebridgesgroup.org.uk) or from the Group Administrator on 01926 812383 or admin@thebridgesgroup.org.uk.

You can withdraw or change your consent at any time by contacting the Group Administrator (see above). 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.

Please return this form by email to admin@thebridgesgroup.org.uk (the email will be kept as part of your consent) or by post to the Group Administrator, c/o Sycamore Lodge, Church Street, Stockton, Southam, CV47 8JG or via your churchwarden to the Group Administrator.

The Bridges Group of Parishes

Lower Shuckburgh, Napton & Stockton, with Priors Marston, Priors Hardwick & Wormleighton

Data Privacy Notice

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 separate PCCS and Priest-in-Charge of the Bridges Group of Parishes are the data controllers. This means they decide how your personal data is processed and for what purposes.

3. How do we process your personal data?

The Bridges Group of Parishes 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 across our six parishes;
- To administer membership records;
- 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, services and initiatives across the Group;

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

There are several lawful bases for us processing your personal data, including:

- You have given us explicit consent so that we can keep you informed about local news, events, activities, services and initiatives.
- Processing is necessary for carrying out legal obligations e.g. in relation to Gift Aid or compliance with the Church Representation Rules;
- Processing is carried out by us as a not-for-profit body with a religious aim in our legitimate activities.

5. Sharing your personal data

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

6. How long do we keep your personal data[1]?
We keep data in accordance with the guidance set out in the guide "Keep or Bin: Care of Your Parish Records" which is available from the Church of England website [see footnote for link].

Specifically, we retain electoral roll data while it is still current; gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and parish 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:

- To request a copy of your personal data which the Bridges Group holds about you;
- To request that the Bridges Group corrects any personal data if it is found to be inaccurate or out of date;
- To request your personal data is erased where it is no longer necessary for the Bridges Group to retain such data;
- To withdraw your consent to the processing at any time;
- To request a restriction is placed on further processing where there is a dispute in relation to the accuracy or processing of your personal data;
- To object to the processing of personal data 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;
- To lodge a complaint with the Information Commissioners Office.

8. 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.

9. Contact Details
To exercise all relevant rights, queries of complaints please in the first instance contact the Group Administrator on 01926 812383 or admin@thebridgesgroup.org.uk.

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.

[1] Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/more/libraries-and-archives/records-management-guides

Appendix D

The Bridges Group of Parishes

Lower Shuckburgh, Napton & Stockton, with Priors Marston, Priors Hardwick & Wormleighton

Request for personal data under the General Data Protection Regulations 2018

Please complete this form to help us identify all the relevant personal data to which you wish to gain access.

SECTION 1 – Your personal details

Full name: ……..

Former surname: ……..

Address: ……..

……..

……..

Postcode: ……

Landline telephone number: ……..

Mobile telephone number: ……..

Email address: ……

Please give us details of your previous address if you have not lived at your current address for two years or more:

Address: ……..

……..

……..

Postcode: ……

Please continue to next page

SECTION 2 – Details of data

Please describe in as much detail as possible the information you are requesting and all the church bodies you think may be holding your data, together with offices or posts you held and other reasons you think data is being held.

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

Please continue to next page

SECTION 3 – Additional information required

It is vitally important to us that your personal data is protected and held in accordance with GDPR. To ensure we disclose the information requested only to you, please provide two proofs of identity (one of which must contain a photograph of yourself).

1. ……

2. ……

(Copies of documents will be accepted but we reserve the right to request sight of the originals.)

SECTION 4 – Declaration of Data Subject (the person about whom the data is held)

I confirm that I am seeking access to personal information about myself.

Signed: ……

Date: ……

Please return this form to:

Data Protection Compliance Officer
c/o Sycamore Lodge
Church Street
Stockton
Southam CV47 8JG

or via email to: admin@thebridgesgroup.org.uk

For office use only

Date form received:	
One month expires:	
ID received and checked:	
Request referred to:	
Date of referral:	
Reason request refused (if applicable):	
Fee charged (if applicable):	
Date fee received:	
Date of response to data subject:	
Any other action:	

RETENTION GUIDELINES

The following retention guidelines give suggested minimum periods for keeping each type of parish record less than 100 years old. If you are in any doubt please seek advice from your Diocesan Record Office, which is usually your local Archives and Local History Service.

Key:

- Deposit: at the Diocesan Record Office/Registry. Important material which needs to be kept permanently. It is acceptable to deposit originals with the Diocesan Record Office or Diocesan Registry.
- Destroy: Ephemeral material which can be discarded once its purpose has been served. Do not destroy if there is any possibility that the document may be required as evidence.
- Review/Sample: Material where a proportion needs to be kept, either by reviewing its value after an agreed period, or by taking a sample. Where it is appropriate transfer the whole record series to the Local Record Office to allow the archivists there to take an appropriate sample.

Basic Record description	Keep in parish	Final action
CHURCH SERVICES Baptism, marriage, burial, and confirmation registers	Arrange phased transfer to the Archives and Local History Service	Permanent (deposit)
Banns registers	Arrange phased transfer to the Archives and Local History Service	Permanent (deposit)
Service registers	Arrange phased transfer to the Archives and Local History Service	Permanent (deposit)
Orders of service	Arrange phased transfer to the Archives and Local History Service	Permanent (deposit)
Baptism certificate counterfoils; marriage certificate counterfoils; copy burial and cremation certificates; applications for baptisms, banns and marriages	Last entry + 2 years	Destroy
CHURCH BUILDINGS AND PROPERTY **Fabric and furnishings** Faculties, citations and accompanying records	Last action + 5 years	Permanent (deposit)
Terrier and inventory, logbook	Last action + 1 year	Permanent (deposit)
Architect's Quinquennial reports	Last action + 5 years	Permanent (deposit)
Minutes, accounts, specifications, tenders, contracts, plans, photographs, drawings and other papers relating to major works to the church	Last action + 5 years	Permanent (deposit)
Contracts, tenders and specifications for minor works	Last action + 6 years	Destroy
Organ specifications, contracts, papers	Last action + 5 years	Permanent (deposit)
Parsonage House Plans, photographs, drawings	Last action + 5 years	Review for possible deposit

Minutes, accounts, specifications, tenders, contracts, plans, photographs, drawings and other papers relating to major works to the parsonage house	Last action + 5 years	Review for possible deposit
Contracts, tenders and specifications for minor works	Last action + 5 years	Destroy
Quinquennial reports	Last action + 5 years	Review for possible deposit
Churchyard Plans, registers of graves, faculties, citations and accompanying records	Last action + 5 years	Permanent (deposit)
Agreements concerning maintenance of churchyard, graves and memorials	Last action + 5 years	Permanent (deposit)
Minutes, accounts, specifications, tenders, contracts, plans, photographs, drawings and other papers relating to major works to the churchyard	Last action + 5 years	Permanent (deposit)
Contracts, tenders and specifications for minor works	Last action + 6 years	Destroy
GENERAL PARISH ADMINISTRATION **Incumbent and other ministers** Institutions, admissions, licences	Current year + 6 years	Review for possible deposit
Correspondence concerning appointments	Last action + 5 years	Review/Sample
Union of Benefice papers, pastoral schemes and orders; plurality orders; documents establishing team or group councils; Joint PCCs or District Church Councils, and relevant papers and correspondence	Last action + 5 years	Permanent (deposit)
Ministers' papers relating to major parish developments or parish audits	Last action + 5 years	Permanent (deposit)
Ministers' correspondence and other papers on routine administration	Current year + 3 years	Destroy
Maps of parish boundaries, street lists	Last action + 5 years	Permanent (deposit)
Copies of replies to questionnaires or important circulars	Last action + 5 years	Permanent (deposit)
Parochial Church Councils, Team and Group Councils, District Church Councils, etc; Churchwardens and other parish officers Minutes of Council and Committees, Parochial Church Meetings, and Meetings of Parishioners for Appointment of Churchwardens	Last action + 5 years	Permanent (deposit)
Electoral rolls	Last complete review + 6 years	Review/Sample
Parish profiles on vacancy in benefice	Last action + 5 years	Permanent (deposit)
Visitation papers	Last action + 5 years	Permanent (deposit)

Copies of replies to Articles of Enquiry	Last action + 5 years	Permanent (deposit)
Sequestration records	Current year + 6 years	Review/Sample
Visitors' books	Last entry + 3 years	Destroy
Routine correspondence	Current year + 3 years	Destroy
Copies of circulars sent by other organisations, non-local material	Current year + 1 year	Destroy
PARISH FINANCE Annual audited accounts	Current year + 6 years	Permanent (deposit)
Cash books, bills, vouchers, bank statements, other subsidiary financial records	Current year + 6 years	Destroy
Planned giving schemes	Current year + 6 years	Destroy
Gift aid declarations	Keep as long as they are valid + 6 years	Destroy
Insurance policies – employers' liability	Current year + 40 years	Destroy
Insurance policies – other than employers' liability	Current year + 6 years	Destroy
Church copyright licence information	Current year + 6 years	Review/Sample
PASTORAL CARE, SAFEGUARDING AND HEALTH AND SAFETY Accident reporting sheets or book – if relating to adults	Date of incident + 20 years	Destroy
Accident reporting sheets or book – if relating to children	The date when a child became an adult + 20 years	Destroy
A clear Criminal Records Bureau (CRB) or DBS certificate or disclosure letter of confirmation.	Within 6 months of the recruitment decision	Destroy
Risk assessment recommendations and management plan in the event of an unclear or blemished CRB/DBS disclosure.	50 years after appointment/employment ceases	Destroy
Records of other safeguarding adult or child protection incidents either within the parish or within a family/by an individual where the Parish was the reporting body or involved in care or monitoring plans. That is, any sex offender risk assessments and monitoring agreements.	50 years after the conclusion of the matter.	Destroy
Records of any children's activities, Sunday school/ junior church/youth club registers and related general safety risk assessments. Any communication from parents or other parties in relation to the above.	50 years after the activity ceases.	Destroy
Personnel records relating to lay employees not working with children and vulnerable adults: including annual performance assessments, disciplinary matters, job descriptions, training and termination documentation.	6 years after employment ceases	Destroy
Personnel records with contact with children and vulnerable adults including all	50 years after the conclusion of the matter.	Destroy

documentation concerning any allegations and investigation regardless of the findings.		
Parish agreement with the diocese on Obtaining CRB/DBS Disclosures.	Last action + 5 years	Permanent (deposit)
LEGAL DOCUMENTS Deeds, Local Ecumenical Partnership agreements, statutory documents etc; title deeds, other documents relating to title, acquisition, disposal, or rights over a property; statutory notices, orders etc, including Orders in Council for closure of churchyard; and relevant correspondence	For all documents in this category, consult the Diocesan Registrar	Permanent (deposit)
Charities: deeds, schemes, orders, minutes, accounts, distribution lists, benefactions	Consult Trustees' Solicitor	Permanent (deposit)
OTHER PARISH RECORDS Public Notices	Current year + 5 years	Consider sampling
Rota/duty lists	Current year + 2 years	Destroy
Routine correspondence	Current year + 6 years	Destroy
PARISH ORGANISATIONS **M.U., Youth Clubs, choir, bell- ringers etc** Minutes, reports, accounts	Last action + 5 years	Permanent (deposit)
Membership lists	Last action + 5 years	Destroy
Correspondence and contracts	Current year + 6 years	Review/Sample
Choir register	Current year + 3 years	Review/Sample
Music lists	Current year + 3 years	Review/Sample
PUBLICATIONS Bibles, Communion Books, Hymn Books, Prayer Books, Psalters and Service Books.	Replace with new versions	Consider keeping one sample copy on replacement
Altar and desk editions of the Bible, Common Book of Prayer and Common Worship	Replace with new versions	Permanently retain in the parish
Church Guides and Parish Histories	Replace with new versions	Permanent (deposit)
Parish magazines	Last action + 5 years	Permanent (deposit)
Scrapbooks, newspaper cuttings, brochures, record of gifts, photographs	Last action + 5 years	Permanent (deposit)

Extract from:
"Keep or bin….? The care of your records"
Church of England Record Centre
Records Management Guide No. 1
Revised 2009
Records Management Guides from the Church of England
Downloaded from Church of England website
17/04/18