



# CAVERSHAM THAMESIDE AND MAPLEDURHAM

ST PETER | ST MARGARET | ST JOHN

## Data Protection Policy

### Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Purpose.....	2
1.2	Scope.....	2
1.3	Definitions.....	2
<b>2</b>	<b>Policy Statement.....</b>	<b>3</b>
2.1	Data Protection Lead.....	3
2.2	Principles of data protection.....	3
2.3	Collecting personal data.....	4
2.4	Privacy Notice.....	4
2.5	Lawful bases.....	5
2.6	Individual rights.....	5
2.7	Data Protection Impact Assessment.....	5
2.8	Data Sharing.....	5
2.9	Storing and disposing of data.....	6
2.10	Fact versus Opinion.....	6
2.11	Data Breaches.....	7
2.12	Training.....	7
<b>3</b>	<b>Approval and review.....</b>	<b>7</b>
<b>4</b>	<b>Revision History.....</b>	<b>7</b>
<b>5</b>	<b>APPENDIX 1 – Lawful bases (from GDPR Article 6).....</b>	<b>7</b>
<b>6</b>	<b>APPENDIX 2 - Information Asset Register.....</b>	<b>8</b>
<b>7</b>	<b>APPENDIX 3 – Register of Processing Activities.....</b>	<b>12</b>
<b>8</b>	<b>APPENDIX 4 – Retention schedule.....</b>	<b>23</b>

## 1 Introduction

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that the Parish of Caversham Thameside and Mapledurham takes seriously. Embedding data protection within the organisation benefits the Parish of Caversham Thameside and Mapledurham, the Church and all

individuals who interact with us, by enabling uniform and consistent decision making, building a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through transparency and accountability, instilling trust and confidence in individuals when they provide us with their data, and ensuring their rights and freedoms are upheld.

### 1.1 Purpose

The purpose of this policy is to describe the steps that the Parish of Caversham Thameside and Mapledurham are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable.

This policy is also intended to provide us with measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals being uninformed by lack of transparency leading to unlawful practice;
- the invasion of privacy due to over-collection or over-retention of data.

### 1.2 Scope

This policy applies to the Parish of Caversham Thameside and Mapledurham, which includes the Parochial Church Council (PCC) and the incumbent, the Rector of Caversham Thameside and Mapledurham.

We expect all those processing personal data on behalf of the Parish of Caversham Thameside and Mapledurham to act in accordance with this policy when engaged in the business of the parish.

#### Joint Data Controllers

The incumbent and PCC have agreed to work as joint data controllers for data protection purposes

### 1.3 Definitions

- **Personal Data** - Any information that relates to an identifiable living individual.
- **Special Categories of Personal Data** (also known as sensitive personal data) - Specific types of data that require additional care being taken when processing. The categories are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.
- **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.
- **Data Protection Impact Assessment (DPIA)** - A process designed to help systematically analyse, identify and minimise the data protection risks of a project or activity.
- **Data Subject** - The individual to whom the data being processed relates.
- **Data Controller** - A body or organisation that makes decisions on how personal data is being processed. Data Controllers almost always also process data.

- **Data breach** - any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction).
- **3rd Party Data Processors** – Other legal entities that process data on behalf of a Data Controller and under instruction from the Data Controller. Data Processors do not have the ability to make decisions about *how* the data should be processed, there should be documented instructions from the Data Controller about what the processor can and cannot do with the data (known as a Data Processing/Sharing Agreement).

## 2 Policy Statement

Personal data that the Parish of Caversham Thameside and Mapledurham collects, uses, stores, transfers, shares and disposes of must be handled in line with the following policy.

### 2.1 Data Protection Lead

The Parish of Caversham Thameside and Mapledurham has a Data Protection Officer (DPO), based at the Parish Office, Church House, 59 Church Street, Caversham, Reading RG4 8AX who may also be contacted by emailing: [dataprotection@ctmparish.org.uk](mailto:dataprotection@ctmparish.org.uk) or by phoning: 0118 947 1703.

They are responsible for assisting the Parish of Caversham Thameside and Mapledurham to monitor internal compliance and to inform and advise on data protection obligations.

They will monitor data sharing agreements, data breaches, information risk, subject access requests and compliance with data protection policies and procedures. They will report to the PCC.

### 2.2 Principles of data protection

Personal data is processed according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject, through the provision of clear and transparent privacy notices and responses to individual rights requests.
2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes. The Parish of Caversham Thameside and Mapledurham will maintain an Information Asset Register (Appendix 2) and Register of Processing Activities (Appendix 3) for the parish that will be regularly and consistently reviewed and updated. Data that is stored and used for archiving purposes in the public interest, scientific or historical research or statistical purposes will be managed by and stored at the Berkshire Records Office and Oxfordshire Records Office
3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to regular review of data collection and processing needs.
4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular data quality checks.
5. **Data is not kept for longer than is necessary** to complete the task for which it was collected, by the implementation of a retention schedule (Appendix 4) and a regular data cleansing programme.

6. **Data is kept secure**, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, accidental corruption, loss or disclosure of personal data. This will include:
- storing paper copies of personal data in locked cabinets;
  - maintaining password protection of electronic data held on computers and online storage;
  - ensuring access to paper and electronic media is restricted only to those individuals authorised to access the data;
  - ensuring that extra precautions are taken when personal data is carried in public places, to keep the risk of data breaches to an acceptable level.

To maintain appropriate data security, we will undertake regular risk assessments of our practices and provide awareness and training to all those processing personal data on behalf of the parish.

7. **Data that is transferred outside the European Union** will only take place with appropriate safeguards to protect the rights of individuals.
8. **Accountability.** The Parish of Caversham Thameside and Mapledurham are responsible for, and will demonstrate, compliance with the principles by:
- Adopting and implementing this data protection policy;
  - Publish privacy notices to explain our data protection practices to those whose personal data we process
  - Put in place written contracts with 3rd party Data Processors that process personal data on our behalf;
  - Implementing annual reviews, to update the measures we have put in place.

## 2.3 Collecting personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. If we acquire any personal data related to an individual (including employees, officer holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, we must do so in line with the above 'Principles of Data Protection'.

If we acquire data in error (that is, data we should not have access to), by whatever means, we must inform the Data Protection Lead who will assess whether the data should be retained and if so, arrange for it to be given to the appropriate individual.

## 2.4 Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data and the Parish of Caversham Thameside and Mapledurham will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice can be found here: [www.ctmparish.org.uk/wp-content/uploads/2018/05/2018\\_Data\\_privacy\\_notice.pdf](http://www.ctmparish.org.uk/wp-content/uploads/2018/05/2018_Data_privacy_notice.pdf).

We shall create and maintain one or more privacy notices, covering our data processing activities relating to personal data. Privacy notice(s) will be published on our website and we will provide this to individuals at the time we collect or significantly amend their personal data.

If our data processing practices change, causing a Privacy Notice to be updated, we will reissue the notice to the affected data subjects, by email.

## 2.5 Lawful bases

Personal data must only be processed once we have identified an appropriate lawful reason to do so. There are six available lawful bases for processing (Appendix 1). No single basis is 'better' or more important than the others, we must decide which basis is most appropriate depending on our purpose and relationship with the individual.

The Lawful basis for different areas of our data processing will be included in Appendix 3 of this policy and indicated in the relevant Privacy Notice.

## 2.6 Individual rights

Data protection legislation gives individuals specific rights regarding their personal data:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability (unlikely to be relevant to parishes or deaneries)
7. The right to object
8. Rights in relation to automated decision making and profiling (unlikely to be relevant to parishes or deaneries)

## 2.7 Data Protection Impact Assessment

The Parish of Caversham Thameside and Mapledurham has adopted the principle of privacy by design. All new projects, updated processes or significantly changed systems that require the use of personal data and may pose a high risk to data subjects, will be subject to a Data Protection Impact Assessment (DPIA). A DPIA template is available here:

<https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf>.

## 2.8 Data Sharing

As a data controller, we recognise that when we share personal data with third parties, we are responsible for:

- ensuring the third party complies with GDPR, and
- stating any constraints or requirements about what the third party can or cannot do with our data.

When sharing or disclosing personal data we shall ensure that:

- We consider the benefits and risks, either to individuals or the Church, of sharing the data, along with the potential results of not sharing the data;

- We are clear about with whom we can share the data. If we are unsure, we check with the data owner, or our Data Protection Lead person.
- We do not disclose personal data about an individual to an external organisation without first checking that we have a legitimate reason to do so (see above 'Lawful bases' section).
- If we must transfer or share data, we do so using appropriate security measures;
- If we are sharing data outside of the UK or the EU, we take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

If we are unsure whether or not we can share information, we will contact our Data Protection Lead person.

### Data Sharing statements

We may state any constraints or requirements on the use of data shared with third parties in the following ways, depending on the level of risk:

- Through the use of disclaimer-type statements in emails or on contractor job sheets
- By the inclusion of a 'Data Protection' section of a contract with a third party (such as a leasing agreement)
- By a standalone 'Data Sharing Agreement'

## 2.9 Storing and disposing of data

We will ensure that we use the most appropriate and secure methods available for both storage and disposal of personal data. We will ensure that:

- In so far as we are able, all personal data in our possession is kept secure from unauthorised access;
- We lock physical files containing personal data in a secure cabinet;
- We are vigilant of our surroundings, in particular when working outside of normal office locations, being careful not to place any personal data in a position where it can be viewed, stolen or lost;
- All devices used to handle personal data are password protected and we do not share passwords;
- Desks are kept clear of personal data when not occupied.

## 2.10 Fact versus Opinion

When using personal data, it is our policy not to write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. In general we:

- Express facts, not opinions
- Work on the basis that anything written about an individual might be seen by that individual.

This includes emails. Although a certain amount of informality attaches to email writing, it should not be overlooked that these can provide a written record of our comments and, in the event of a Subject Access Request, they are subject to disclosure if they contain personal data.

## 2.11 Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Any data breach, as described above, is to be reported to the Data Protection Lead person.

Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, our Data Protection Lead person will report this to the ICO within 72 hours and will co-operate with any subsequent investigation. We will contact the affected data subject(s) where it is necessary to do so.

## 2.12 Training

We will provide appropriate support and training to all those involved in the parish in the safe and lawful processing of personal data.

## 3 Approval and review

Approved by	Parochial Church Council
Policy owner	Caroline Smith
Policy author	Mike Smith & Caroline Smith
Date	21/11/19
Review date	1 year

## 4 Revision History

Version No	Revision Date	Previous revision date	Summary of Changes
2020 11 18	18/11/20	n/a	none

## 5 APPENDIX 1 – Lawful bases (from GDPR Article 6)

### Legitimate interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate Interest Assessment. When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject

- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

### Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

### Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

### Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

If Consent is used it must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded.

For consent to be valid, i.e. the correct basis, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g. pension, payroll etc) then the data controller cannot refuse the service, so there is effectively no choice, so consent is not valid.

### Vital interests

The processing is necessary to protect someone's life.

### Public Task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

For further information and assistance seek advice from [the DPO or Data Protection Lead or local registrar as appropriate].

## 6 APPENDIX 2 - Information Asset Register

No.	Title and description	Storage: location and format	Sensitivity of data (risk)
1	Gift Aid Declarations	password protected PCs belonging to church treasurers/ church giving officer	high
2	Parish Directory	password protected PC. Parish Administrator only	medium

Data Protection Policy

No.	Title and description	Storage: location and format	Sensitivity of data (risk)
3	Rector's contact list	password protected PC. Held by Parish Administrator and shared with clergy	high
4	Fete Raffle	Held by person running raffle on fete committee	high
5	Fete programme advertisers	Fete Committee comms person. Kept on personal laptop	high
6	Caversham Church Fete service providers	Fete Committee comms person. Kept on personal laptop	
7	Electoral Roll	held on password protected pc. Parish Administrator only can access	low
8	Baptism forms	Soft copies on password protected pcs. Clergy & admin team only can access. Hard copies in safe/vestry/clergy offices	medium
9	Baptism follow-up	held on password protected pc. Parish Administrator & clergy team can access	medium
10	Wedding forms	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, copy at church in locked safe, hard copy with minister	medium
11	Banns forms	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, copy at church in locked safe	medium
12	Funeral forms	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, hard copy with minister	medium
13	Funeral follow-up	password protected pc. Parish Administrator maintains	medium
14	St Peter Sunday Club Register of attendance	folder in cupboard in locked vestry	medium
15	St John's Sunday Club details	locked cupboard in church	high
16	St Margaret's Junior Church	in church safe	high
17	Safeguarding cases	Rector only. Soft copy – Password protected Hard copy – kept in lock cabinet	high
18	Committee member list (PCC/CLT)	PCC secretary, CLT secretaries, clergy. Password protected PCs	medium
19	Church Rotas (Vestry duty, coffee rota, serving etc)	rota manager and rota members. Password protected PCs	medium

Data Protection Policy

No.	Title and description	Storage: location and format	Sensitivity of data (risk)
20	Parish Grants Applications	Committee members only. password-protected computer and paper copies kept in locked filing cabinet	medium
21	Church House bookings	Parish Secretary only. Soft copy – Password protected. Hard copy – kept in locked office	medium
22	Church bookings	Parish Secretary and churchwardens plus those hosting visitors. Soft copy – Password protected. Hard copy – kept in locked office	medium
23	DBS & referencing	Parish Administrator only. Soft copy – Password protected Hard copy – kept in locked office	high
24	Parish employees	Hard copies kept in locked offices. Soft copies on clergy password protected PCs	high
25	Recruitment candidates	soft & hard copies held by Parish Administrator, clergy as appropriate	high
26	Children's Society box holders	Local administrator. Hard copy only, securely stored	high
27	Media contacts list	Digital. Kept on personal laptop of media officer	medium
28	Amersham Road Cooking Club.	Data is held on paper – registration forms and also on a database, kept at the house of one of the ARCC core team on a password-protected PC	high
29	St John's Keyholders' list	list manager only can access. password protected computer & locked filing cabinet	medium
30	St John's Rotas: servers, chalice assistants, intercessors, cleaning	rota manager controls on password protected computer	medium
31	St John's Updates	church minister. On password protected pc	medium
32	St Peter's Updates	churchwarden. password protected pc	medium
33	St Peter's Junior choir	Held by Junior choir leader. 1 copy at home 1 copy in the choir vestry. Also emergency phone numbers kept in choir vestry.	medium
34	St Peter's adult choir	choir director only. password protected pc	medium
35	St Peter's completed blue envelopes	Gift Aid Officer then Parish Administrator for storage. Gift Aid officer's house then locked office	high

Data Protection Policy

No.	Title and description	Storage: location and format	Sensitivity of data (risk)
36	St Peter's key holders	hardcopy only held in locked office	low
37	St Peter's church rotas	rota manager and rota members. Password protected PCs	low
38	St Margaret's church rotas	rota manager and rota members. Password protected PCs	low
39	St Peter's & St Margaret's Bellringers	Held on Tower Secretary's computer only. ODG members on tower treasurer's pc	medium
40	St Peter's & St Margaret's Bellringers Child registration record	On paper, filed in tower in locked box	high
41	St Peter's & St Margaret's Bellringers Attendance record - adult and child	Hard copy; kept in tower. Only ringers have access	
42	St John's CLT members list	Minister. password protected pc	medium
43	PCC member list	PCC secretary. Password protected pc	medium
44	St John's small group members list	Minister password protected pc	low

## 7 APPENDIX 3 – Register of Processing Activities

The table below is accurate at the date of approval of this policy. From time to time this register may be update, and the up to date version can be obtained from the Parish Administrator

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Gift Aid Declarations	claim Gift Aid from the Government	name and address	members of the congregation	claiming Gift Aid. Legal obligation	password protected PCs belonging to church treasurers/ church giving officer	HMRC	Six complete calendar years after last gift claimed on the declaration
Parish Directory	make contact details available	names, address, phone numbers, email addresses	members of the congregations	making a directory. Consent	password protected PC. Parish Administrator only	none	one year
Rector's contact list	keep in touch	names, address, phone numbers, email addresses	members of the congregations and others	Contacting members of the parish. Consent	password protected PC. Held by Parish Administrator and shared with clergy	none	whist current

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Fete Raffle	fund raising	Names and addresses to send raffle tickets to previous supporters	from the individuals on the list	Consent	Held by person running raffle on fete committee	none	Until people ask not to be on the list
Fete programme advertisers	fund raising	list of local companies and their contact details	from the advertisers	contractual	Fete Committee comms person. Kept on personal laptop	printers only	whist current
Caversham Church Fete service providers	fund raising	names and contact details of individuals and companies	from the individuals on the list. Consent	contractual	Fete Committee comms person. Kept on personal laptop	none	whist current
Electoral Roll	Parish Electoral Roll	names and address only	members of the congregations	making and keeping an Electoral Roll as required by the Church of England. Legal obligation	held on password protected pc. Parish Administrator only can access	none	6 years (until roll is rewritten). Shredded
Baptism forms	Baptism	names, addresses, phone numbers, email addresses, dob of child	baptism families	details for the baptism register and pastoral follow up. Legitimate interest	Soft copies on password protected pcs. Clergy & admin team only can access. Hard copies in safe/vestry/clergy offices	none	in registers held in perpetuity on PC & hardcopy - 2 years then shredded

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Baptism follow-up	pastoral care	names, address, phone numbers, email addresses	baptism families	pastoral care and to invite people to specific events. Consent	held on password protected pc. Parish Administrator & clergy team can access	none	until consent is withdrawn. Shredded
Wedding forms	to record details required by law for marriage registers	Info for the register & documentary evidence of ID	from wedding couples	legal requirement to collect details and confirm identity. Legal obligation	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, copy at church in locked safe, hard copy with minister	quarterly return to the local Register Offices (Reading & Henley)	Parish Administrator - 2 years Churches and clergy until after wedding
Banns forms	to record details required by law for banns registers	Info for the register	from the couple getting married (in another parish)	legal requirement to collect details. Legal obligation	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, copy at church in locked safe	the church where the couple are marrying in form of a banns certificate	Parish Administrator - 2 years Churches and clergy until after banns have been read

Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Funeral forms	Pastoral information for clergy & parish registers	names, address, phone numbers, email addresses	funeral directors	Legitimate interest	soft copy on password protected pc. Hard copy with Parish Administrator in locked office, hard copy with minister	none	Parish Administrator - 2 years. Ministers until after funeral. Shredded.
Funeral follow-up	pastoral care	names, address, phone numbers, email addresses	funeral directors	Pastoral care and to invite people to specific event, including All Souls. Consent	password protected pc. Parish Administrator maintains	none	until consent is withdrawn. Shredded
St Peter Sunday Club Register of attendance	safeguarding of children	first names only	parents	keeping track of who attends sessions. Legal obligation	folder in cupboard in locked vestry	none	25 years. Shredded
St John's Sunday Club	safeguarding of children	children's details inc medical, parental contact info, photo permission, consent to receive email updates	parents	keeping track of who attends sessions. Legal obligation	locked cupboard in church	none	25 years. Shredded

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
St Margaret's Junior Church	safeguarding of children	children's details inc medical, parental contact info	parents	keeping track of who attends sessions. Legal obligation	folder in church safe	none	
Safeguarding cases	maintain records on current and historic safeguarding cases	names and pastoral details	individuals concerned, diocesan & statutory bodies	legal obligation	Rector only. Soft copy – Password protected Hard copy – kept in lock cabinet	diocese and statutory bodies as required	In perpetuity
Committee member list (PCC/CLT)	contact purposes	names, address, phone numbers, email addresses	committee members themselves	Contact purposes. Legitimate interest	PCC secretary, CLT secretaries, clergy. Password protected PCs	none	while the person is serving on the PCC then deleted
Church Rotas (Vestry duty, coffee rota, serving etc)	contact purposes	names, address, phone numbers, email addresses	people on the rotas plus clergy	to facilitate the rota. Legitimate interest	rota manager and rota members. Password protected PCs	none	whilst current
Parish Grants Applications	fund raising	project funding applications inc personal details of applicant	those apply for grants	Legitimate interest	Committee members only. password-protected computer and paper copies kept in locked filing cabinet	none	7 years shredded/ deleted

Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Church House bookings	Church House bookings	names, address, phone numbers, email addresses	groups/individuals who are making bookings	information on room hirers. Contractual	Parish Secretary only. Soft copy – Password protected Hard copy – kept in locked office	none	7 years shredded/ deleted
Church bookings	Church bookings	names, address, phone numbers, email addresses	groups/individuals who are making bookings	Information on hirers. Contractual	Parish Secretary and churchwardens plus those hosting visitors. Soft copy – Password protected Hard copy – kept in locked office	none	7 years shredded/ deleted
DBS & referencing	to complete checks on all volunteers working with children and vulnerable adults	person data, potentially sensitive	from individuals and from DSBS checking Co	data is used to confirm individual can take the post they are interested in. legal obligation	Parish Administrator only. Soft copy – Password protected Hard copy – kept in locked office	none unless there is an adverse DBS check or reference	25 years
Parish employees	employing & managing parish staff	person data, potentially sensitive	employees	Management of employees. Legal obligation	Hard copies kept in locked offices. Soft copies on clergy password protected PCs	none	6 years after employment ceases

Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Recruitment candidates	employing parish staff	person data, potentially sensitive	candidates for interview	Facilitating recruitment. legitimate interest	soft & hard copies held by Parish Administrator, clergy as appropriate	none	shredded/ deleted at end of recruitment process
Children's Society box holders	For the official record of box collections as requested by the Society. Boxholders have entered into a contract with The Children's Society through the Box Secretary	Contact details and amount collected	individuals concerned	Fund raising. Legitimate interest	Local administrator. Hard copy only, securely stored	Children's Society	For six years after last counted and receipted
Media contacts list	distributing news and information relevant to the media	email addresses and phone number	local news outlets	legitimate interest	Digital. Kept on personal laptop of media officer	none	whilst current

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
Amersham Road Cooking Club	maintain membership list	Details of children attending the club, and their parental contacts	parents/guardians	Legal obligation & Consent	Data is held on paper – registration forms and also on a database, kept at the house of one of the ARCC core team on a password-protected PC	none	25 years
St John's Keyholders' list	keyholder list	names only	individuals	Legitimate interest	List manager only can access. password protected computer & locked filing cabinet	none	Whilst current. Deleted from spreadsheet
St John's Rotas: servers, chalice assistants, intercessors, cleaning	facilitate the running of church	contact details	people on the rota	To facilitate the rota. Legitimate interest	rota manager controls on password protected computer	none	Whilst current. Deleted from spreadsheet
St John's Updates	regular updates to church members	information on events and services	individuals	emailing church members. Consent	church minister. On password protected pc	none	until consent is withdrawn
St Peter's Updates	regular updates to church members	information on events and services	individuals	emailing church members. Consent	churchwarden. password protected pc	none	until consent is withdrawn

Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
St Peter's Junior choir	manage junior choir membership	child details and parental contact information	parents	keeping track of who attends sessions. Legal obligation	Held by Junior choir leader. 1 copy at home, 1 copy in locked cupboard in choir vestry	none	25 years
St Peter's adult choir	contact one another with information about music in church and choir	contact details	individuals	to enable choir members to contact one another. Legitimate interest	choir director only. password protected pc	none	whilst current
St Peter's completed blue envelopes	managing donation scheme	contact details and donation amounts	donors	keeping track of donations. Legitimate interest	Gift Aid Officer then Parish Administrator for storage. Gift Aid officer's house then locked office	HMRC	7 years (financial), then shredded/deleted
St Peter's key holders	list of people who hold keys for St Peter's Church	name only	from the individual who holds the key(s)	list all people who can access the church. Legitimate interest	hardcopy only held in locked office	none	once key is relinquished. Form shredded

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
St Peter's church rotas	managing rotas for chalice assistants, vestry team, coffee team, intercessors, readers, servers, sidespeople	name and contact details. Name only displayed in church on hard copy	individuals	facilitating rotas. Legitimate interest	rota manager and rota members. Password protected PCs	none	whilst current
St Margaret's church rotas	managing rotas for coffee team & readers	name and contact details	individuals	facilitating rotas. Legitimate interest	rota manager and rota members. Password protected PCs	none	whilst current
St Peter's & St Margaret's Bellringers	bellringers contact information	Email addresses, phone numbers and home addresses of regular ringers inc ODG membership subscription	individuals	Arranging bell ringing and distribution of notices (including, e.g. those from Guild and Branch). Legitimate interest	Held on Tower Secretary's computer only. ODG members on tower treasurer's pc	Oxfordshire Guild of Bellringers	whilst person remains in ringing band and for 6 years after last payment in line with accounting requirements (ODG membership)
St Peter's & St Margaret's Bellringers Child registration record	Bellringers Child registration record	child details and parental contact information	parents	Compliance with Child Safeguarding Procedures. Legal obligation	On paper, filed in tower in locked box	none	until they turn 18 or leave then take to parish central filing

## Data Protection Policy

<i>Description</i>	<i>Reason/purpose: What are you trying to do &amp; why?</i>	<i>Data Categories: What kind of data is involved. Is it sensitive? Special category?</i>	<i>Collection Point: Where does the data come from?</i>	<i>Processing Justification: What are you doing with this data, and why, including the lawful basis for processing</i>	<i>Database, Location &amp; Access: What, where, who can access &amp; how maintained. Secure?</i>	<i>Data Sharing: which, if any, other organisations (legal entities) do you share this data with?</i>	<i>Retention Policy: How long do you keep the data and how is it deleted/destroyed?</i>
St Peter's & St Margaret's Bellringers Attendance record - adult and child	Bellringers Attendance record - adult and child	names only	the members	Compliance with Child Safeguarding Procedures. Legal obligation	Hard copy; kept in tower. Only ringers have access	none	2 years then take to parish central filing
St John's CLT members list	Maintain membership list	names and contact details of individuals	CLT members	Keep members in contact with one another. Legitimate interest	Minister. password protected pc	none	whilst person is a CLT member
PCC member list	Maintain membership list	names and contact details of individuals	PCC members	Keep members in contact with one another. Legitimate interest	PCC secretary. Password protected pc	none	whilst person is a PCC member
St John's small group members list	Contacting small group members	names and contact details of individuals	group members	Contacting small group members. Legitimate interest	Minister password protected pc	none	whilst current
St John's Alpha course	contacting course participants	names and contact details of individuals	attendees from the course	Group members' details needed for contact during the course and follow up. Legitimate interest	Minister password protected pc	none	whilst current

## 8 APPENDIX 4 – Retention schedule

Description	Retention Policy: How long do you keep the data and how is it deleted/destroyed?
Gift Aid Declarations	Six complete calendar years after last gift claimed on the declaration
Parish Directory	one year
Rector's contact list	whilst current
Fete Raffle	Until people ask not to be on the list
Fete programme advertisers	whilst current
Caversham Church Fete service providers	whilst current
Electoral Roll	6 years (until roll is rewritten). Shredded
Baptism forms	in registers held in perpetuity on PC & hardcopy - 2 years then shredded
Baptism follow-up	until consent is withdrawn. Shredded
Wedding forms	Parish Administrator - 2 years Churches and clergy until after wedding
Banns forms	Parish Administrator - 2 years Churches and clergy until after banns have been read
Funerals	Parish Administrator - 2 years. Ministers until after funeral. Shredded.
Funeral follow-up	until consent is withdrawn. Shredded
St Peter Sunday Club Register of attendance	25 years. Shredded
St John's Sunday Club	25 years. Shredded
St Margaret's Junior Church	
Safeguarding cases	In perpetuity
Committee member list (PCC/CLT)	while the person is serving on the PCC then deleted
Church Rotas (Vestry duty, coffee rota, serving etc)	whilst current
Parish Grants Applications	7 years shredded/ deleted
Church House bookings	7 years shredded/ deleted
Church bookings	7 years shredded/ deleted
DBS & referencing	25 years
Parish employees	6 years after employment ceases
Recruitment candidates	shredded/ deleted at end of recruitment process
Children's Society box holders	For six years after last counted and receipted
Media contacts list	whilst current
Amersham Road Cooking Club	25 years
St John's Keyholders' list	whilst current. Deleted from spreadsheet

## Data Protection Policy

Description	Retention Policy: How long do you keep the data and how is it deleted/destroyed?
St John's Rotas: servers, chalice assistants, intercessors, cleaning	whilst current. Deleted from spreadsheet
St John's Updates	until consent is withdrawn
St Peter's Updates	until consent is withdrawn
St Peter's Junior choir	25 years
St Peter's adult choir	whilst current
St Peter's completed blue envelopes	7 years (financial), then shredded/deleted
St Peter's key holders	once key is relinquished. Form shredded
St Peter's church rotas	whilst current
St Margaret's church rotas	whilst current
St Peter's & St Margaret's Bellringers	whilst person remains in ringing band and for 6 years after last payment in line with accounting requirements (ODG membership)
St Peter's & St Margaret's Bellringers Child registration record	until they turn 18 or leave then take to parish central filing
St Peter's & St Margaret's Bellringers Attendance record - adult and child	2 years then take to parish central filing
St John's CLT members list	whilst person is a CLT member
PCC member list	whilst person is a PCC member
St John's small group members list	whilst current
St John's Alpha course	whilst current