St Barnabas Church

The parish church for Emmer Green and Caversham Park

# Data Protection Policy

## Document history

| Version | Date | Author/Editor | Approved by |
|---|---|---|---|
| 1.0 | 03NOV25 | Felicity Chapman / Roger Moore | PCC |
| | | | |
| | | | |
| | | | |

**Next review date:** **November 2026**

**Issued by:**

St Barnabas: the parish church for Emmer Green and Caversham Park
Grove Road, Emmer Green, RG4 8RA
www.saintbarnabas.org.uk
vicar@saintbarnabas.org.uk
0118 947 5214
Registered charity no. 1164759

# Contents

# 1 Introduction

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that St Barnabas Emmer Green and Caversham Park takes seriously. Embedding data protection within the organisation benefits ourselves, 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 St Barnabas 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 Vicar and PCC of the ecclesiastical parish of Emmer Green and Caversham Park, St Barnabas.

We expect all those processing personal data on behalf of parish to act in accordance with this policy when engaged in the business of parish. We provide leaders of church groups with clear guidance on data privacy and protection.

### Joint Data Controllers

The vicar and PCC 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 St Barnabas collects, uses, stores, transfers, shares and disposes of must be handled in line with the following policy.

## 2.1 Data Protection Lead

St Barnabas has a Data Protection Lead, based at St Barnabas church, Grove Road, Emmer Green, Reading RG4 8RA who may also be contacted by emailing: vicar@saintbarnabas.org.uk or by phoning: 0118 947 5214.

They are responsible for assisting St Barnabas 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 incumbent.

## 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. St Barnabas maintains an Information Asset Register (Appendix 2) that will be regularly 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 St Barnabas and stored at the local records office, in Reading.

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.
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.

    From time to time we will undertake risk assessments of our practices and provide awareness and training to those processing personal data on behalf of St Barnabas.
7. **Accountability**. St Barnabas 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
    - Implementing 3-yearly review of this policy, 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. When 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'.

## 2.4 Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data, and St Barnabas will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice can be found here: https://www.saintbarnabas.org.uk/privacy-notice.

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, with a hard copy on the Parish Centre noticeboard.

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.

## 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 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 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 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

  The following is an example of what is meant by 'disclaimer type statement':

  *The attached personal data is provided by [name_of_data_controller] to [third_party_name] for the purposes of [state_the_purpose_here]. To comply with General Data Protection Regulation 2016/679 and the Data Protection Act 2018, this data is only to be used for [insert_name_here] to contact the persons listed in the attached data file for the above stated purpose. You must not share it with any other third party; you must store it securely and take all reasonable steps to prevent its unauthorised access, accidental deletion or corruption. When you no longer need this data, it must be deleted and any paper copies you have made destroyed. Should this data suffer an unauthorised disclosure (data breach), you are to notify [name and contract detail for lead data protection person].*

- By the inclusion of a 'Data Protection' section of a contract with a third party (such as a leasing agreement)

## 2.8 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 use proprietary cloud-based systems for our finance, website and administration systems, which ensures security of our main stores of personal data and reduces the storage of personal data on our own local devices.
- Church officers (who are likely to be handling personal data on church business more often) are encouraged to take advantage of our Microsoft 365 Professional licences, which ensure any personal data is stored in a commercially secure platform, and church-related personal data is not held in private email accounts or devices.
- We lock physical files containing personal data in secure cabinets;
- We are vigilant of our surroundings, in particular when working in public spaces, 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.

## 2.9 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.

## 2.10 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.

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 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.

## 2.11 Training

We will make this document available to all church officers and volunteers who may be affected by this policy (and draw their attention to it), since it contains information about good practice. From time to time we will provide appropriate support and training to those involved in the parish who will have access to personal data (such as via the iKnow system, MyFundAccounting system or who deal with large email distribution lists), in the safe and lawful processing of personal data.

## 2.12 Dealing with access requests

We will deal with any access requests in accordance with the guidance from the ICO, see https://ico.org.uk/for-organisations/advice-for-small-organisations/subject-access-requests-sar/how-to-deal-with-a-request-for-information-a-step-by-step-guide/.

## 2.13 Dealing with complaints

We will deal with any complaints about our collection, storage, and use of personal data in accordance with the guidance form the ICO, see https://ico.org.uk/for-organisations/advice-for-small-organisations/dealing-with-complaints/handling-complaints-a-step-by-step-guide/

# 3 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 our Data Protection Lead in the first instance.

# 4 APPENDIX 2 - Information Asset Register

| No. | Title and description | Data sensitivity | Storage: location and format | Data security |
|---|---|---|---|---|
| 1 | Main personal database of parish contacts http://www.iknowchurch.co.uk/gdpr/ | Medium | iKnow parish administration system (online) | High Third-party |
| 2 | Safeguarding concern records | High | Parish Office (hard copy, held in secure cabinet) | Medium |
| 3 | DBS, role and safeguarding training records www.parishdashboards.org.uk/api/privacy | High | Parish Safeguarding Hub (online [+]) | High Third-party |
| 4 | Finance information (regular supplier data which includes some personal details) www.datadevelopments.co.uk/Privacy-Policy | Medium | MyFundAccounting system (online, managed by third party) | High Third-party |
| 5 | Electoral Roll information | Medium | Forms held in locked cabinet in church office. Spreadsheet (encrypted) held on ER Officer's laptop. | High |
| 5 | Regular giver information | Medium | Treasurer (hard copy, held at Treasurer's home) | Medium |
| 6 | Young people attendance records (e.g. Toddler group) | Medium | Parish Office (hard copy, held in secure cabinet) | Medium |
| 7 | Data Protection consent forms (either paper copies from church, or email printouts received via the website) | Medium | Parish Office (hard copy, held in secure cabinet) | Medium |
| 8 | Baptism, Banns, Marriage, Confirmation and Admission to Holy Communion registers | Medium | Hard copy, stored in the church safe | High |
| 9 | Live stream video www.youtube.com/@stbarnabaschurchemmergreen5994 | Low | Sunday service videos (edited to remove congregation's faces) stored on our YouTube channel | Public Third-party |
| 10 | Facebook page | Low | Facebook direct messages (online)[✤] | High |

[+] We share data with the Parish Safeguarding Hub to meet our legal obligations. This is defined in our service agreement: https://www.safeguardinghubs.org.uk/support-for-parishes/service-agreement/ .

[✤] Facebook page administrators have access to direct messages. This group is restricted to the incumbent, the church wardens, and an administrator.

# 5 APPENDIX 3 - Future considerations

The following items are to be explored for updates to this policy (or other related documents) in the future:

1. **Hirers**: we process certain personal data relating to hirers of the Church Hall / Parish Centre / Church, in order to administer their bookings. We need to review this process in the light of DP requirements.
2. **Leaders of church groups**: we should give consideration to training on best practice for any leaders who may handle personal data in the course of their work as a group leader.
3. **Insurance**: what cover does the PCC's insurance offer for data breaches? And what protection is appropriate for our Data Protection Lead in the event of a complaint?
4. **Pastoral care records**: when we implement the Pastoral Care Assistant team, the relevant processes need to be reviewed in the light of DP requirements for recording visits, safeguarding concerns, etc. and appropriate training provided to Pastoral Care Assistants
5. **End of role / leaving St Barnabas**: we should give consideration to the process to be followed when someone ends a role or leaves the church, to ensure they no longer have access to personal data and they remove/return any personal data held which relates to their role(s).