The Parochial Church Council (PCC) of St Peter and St Paul, Bromley
'Bromley Parish Church'

DATA PROTECTION POLICY

INTRODUCTION

St Peter and St Paul uses personal data of staff, those involved in the life of the church, associates, alumni, clients and contractors to enable effective communication of events and news, church administration, fundraising, safeguarding, volunteer management and pastoral support.

Personal data typically includes:

- General information such as contact details, participation on courses, membership of church groups, inclusion in various rotas;
- Financial information such as donations, Gift Aid tax reclaims and other information required for legal purposes;
- Personal information in order to comply with employment, tax and pension laws which may include (but not limited to) CVs, references, bank details, visas and passport information
- CCTV images within and around the church premises, for the purposes of safety and security;
- For children's and youth events, details related to health & safety information (for example, medical information) as well as child protection records;
- Pastoral records - summary details of salient facts from pastoral meetings which may include sensitive personal information will be recorded only with the explicit consent of the individuals concerned.
- Recording and uploading, or live-streaming services from our church, online, in order to reach out to those who are unable to attend in person, or who wish to participate in our services remotely and communicate events;
- Photography or video capture within services or at specific events or for specific projects.

SCOPE

This policy applies to St Peter and St Paul, Bromley which includes St Peter and St Paul PCC and the Vicar of St Peter and St Paul

STATEMENT OF POLICY

Personal data that St Peter and St Paul collects, uses, stores, transfers, shares and disposes of must be handled in line with the following policy.

The Accounts Manager will act as the point of contact for Data Protection issues but is not a Data Protection Officer within the meaning of the GDPR.

Principles of Data Protection:

Personal data is processed according to the following principles:

1. Data is processed lawfully, fairly and in a transparent manner

2. Data is collected for specified, explicit and legitimate reasons and not further processed for different reasons incompatible with these purposes.
3. Data is adequate, relevant and not more than is necessary to complete the task for which it was collected.
4. Data is accurate and up-to-date and reasonable steps will be taken to ensure this.
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. .
7. Data that is transferred outside the European Union will only take place with appropriate safeguards to protect the rights of individuals.
8. Accountability. St Peter and St Paul are responsible for, and will demonstrate, compliance with the principles

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 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 Accounts Manager who will assess whether the data should be retained and if so, arrange for it to be given to the appropriate individual.

Photography and Filming:

The categories of personal data we collect via media are:

- Image – We may capture your image whilst filming the church service or at specific events.

We also process "special categories" of information that may include:

- Religious belief – By taking part in the service this may indicate religious belief.
- Archiving – certain services may be retained permanently for historic purposes.

Privacy Notices:

Individuals have the right to be informed about the collection and use of their personal data. St Peter and St Paul will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice will be published on our website and in paper copy on the church noticeboard.

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 2).

Individual Rights:

The Act gives individuals specific rights regarding their personal data:

1. The right to be informed
1. The right to access
2. The right to rectification
3. The right to erasure
4. The right to restrict processing
5. The right to data portability
6. The right to object

Data Protection Impact Assessment: St Peter and St Paul 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).

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.

Data Sharing - Media:

We will be sharing photographs and recorded or live-streamed services with the public, by uploading it to social media and other internet sites, such as Zoom, Facebook, Twitter etc.

This means your data may be stored outside the UK. Each platform has its own privacy policy which describes how your data is used and protected.

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 including keeping physical files in a secure cabinet and implementing password protection of devices.

Media Consent:

Wherever possible we will ensure that you know when photography or videography is taking place in the following ways:

- Advance notice of our intention to photograph/film within event booking forms, event information etc.
- Signage at prominent locations, entry and exit points to the event

Once live-streaming or filming has started consent cannot be withdrawn because your data can't be permanently removed from the internet, nor can a group video or photograph be edited to remove your image.

You may be asked to consent on behalf of children aged 16 years or under attending with you. Please consider whether they would want their images to be uploaded to the internet.

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 we would not be able to defend if challenged.

Data Breaches:

Any data breach, defined in Appendix 1, is to be reported to the Accounts Manager.

Training:

We will provide appropriate support and training to all those involved in the safe and lawful processing of personal data at St Peter and St Paul

Signed: ……..(Incumbent)

Date:…….....

APPENDIX 1 – 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).
- **Data Protection Contact**

  The Accounts Manager will act as the point of contact for Data Protection. They are responsible for assisting St Peter and St Paul to monitor internal compliance and to inform and advise on data protection obligations. They can be contacted at Bromley Parish Church. Church Road, Bromley, BR2 0XH or by emailing: vicar@bromleyparishchurch.org

  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.

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

APPENDIX 2 – Data Processing - Lawful Bases (From GDPR Article 6)

1. 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

2. 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.

3. Legal obligation

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

4. 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.

5. Vital interests

The processing is necessary to protect someone's life.

6. 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, in accordance with the Data Protection Act 2018, Schedule 1, Part 2

Appendix 2 – Data Processing - Special Category Data
(From GDPR Article 9)

Special Category data is permitted to be processed by not-for-profit organisations under article 9(2)(d) where :

> *"processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects".*

The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

We may only use your personal data for the uses and purposes set out above unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original use and purposes.