ST BRANDON'S, BRANCEPETH

DATA PROTECTION POLICY

1. Definitions

Personal Data: Information about a living individual which is capable of identifying that individual e.g. names, email addresses, photos.

Processing: Anything done with or to the personal data including storing it.

Data Subject: The person about whom the personal data is processed.

Data Controller: The person or organisation who determines the how and what of data processing in the parish. In the context of St Brandon's this will be the Parochial Church Council (PCC). The Data Controller may delegate day-to-day administration of GDPR obligations to a Data Processing Sub Group.

The Church: St. Brandon's Church Brancepeth, in the Diocese of Durham.

2. Background & Scope

Background

The General Data Protection Regulation (GDPR) came into force on 25th May 2018, replacing the Data Protection Act 1998 and provides individuals with greater rights and protection regarding how their personal data is used by organisations. Churches and parishes must comply with its requirements. It is supplemented by the UK Data Protection Act 2018 and UK-GDPR, which is the method by which the EU GDPR is adopted into UK law.

Scope

St Brandon's recognises the importance of correct and lawful treatment of personal information its processes and holds whether on paper, on computer or any other media. The church fully recognises, endorses and adheres to the fundamental principles of GDPR although at this stage does not consider registration with the Information Commissioner's Office or appointment of a Data Protection Officer necessary due to the limited nature of the church's legitimate data processing interest.

3. Underlying Principles of GDPR as applied to St Brandon's

All personal data shall:

- Be processed fairly, lawfully and transparently.

- Be obtained for the lawful specified purpose above and not processed in any manner incompatible with that purpose.
- Be relevant, adequate and limited to what is necessary in relation to the purposes.
- Be accurate and where necessary kept up to date and, where inaccurate, rectified or erased without delay;
- Be retained only for as long as is necessary.
- Be kept secure from unauthorised and unlawful processing protected against accidental loss, destruction or damage.
- Be processed in accordance with the data subject's rights, specified below.

4. Rights of the Individual Data Subjects.

The rights of individuals under GDPR are as follows;

- The right to be informed about how personal information will be processed. This will be fulfilled through a Privacy Notice made available on the church web site at www.stbrandon.org.uk to which all data subjects providing personal data to the Church will be directed.
- The right to have access to personal information which is held by the church. Such access to be made available within 30 days of any such request to the Data Controller.
- The right to have their personal data corrected or rectified if it is inaccurate. Any third parties to whom the data has been given must be informed of the correction. Data subjects must also be informed of third parties to whom the personal information has been supplied (if any).
- The right to request the deletion or removal of personal data, unless there is an overriding legitimate interest for the Church to continue processing or retention.
- The right to restrict the processing of personal data, unless there is an overriding reason for the Church to continue processing;.
- The right to move, copy or transfer personal data easily from one IT system to another. This right is unlikely to be relevant due to the way in which the church holds and processes an individual's personal data.
- The right to object to processing data, unless the church has an overriding legitimate interest in continuing to process the data.
- The right not to be subjected to a decision based solely on automated processing which produces legal effects or significantly affects the individual; the Church does not use automated processing or profiling so this right is unlikely to be exercised.

It is the Church's policy that personal data relating to children under the age of 13 may only be held with parental or guardian consent, in addition to any other legal basis.

5. Documentation of Processing Activities

As a small organisation, the Church is required to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

The following must be documented for each processing activity:

- The purposes of processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures.

These activities are documented in Appendix 1 to this policy.

6. Complaint by a Data Subject

Where a data subject believes that their rights under GDPR have been infringed by the church, they should be encouraged to raise their concerns in the first instance with the Church.

Notification should be in writing to the secretary of the PCC (as Data Controller) who will bring the matter to the attention of the PCC at the next available meeting or sooner if considered sufficiently urgent, at the discretion of the secretary.

A response to the complainant will be made in writing on behalf of the Data Controller within 14 days of the meeting.

Should the complainant be unsatisfied with the response of the Data Controller, they have the right to notify the Information Commissioner's Office.

Complainants are also entitled to approach the Information Commissioner's office without first notifying the Church. Any correspondence from the ICO will be shared at the next PCC meeting, or circulated to Standing Committee should a more urgent response be required.

7. Data Protection Impact Assessments.

In the event that the church proposes to embark on a project which will require the processing of sensitive personal data on a large scale (e.g. fund raising for a legitimate purpose) a data protection impact assessment (DPIA) should be carried out by the Data Controller.

The DPIA will include:

- A description of the project
- A description of the processing activities and their purpose
- An assessment of the need for the processing and its proportionality
- Any risks which may arise from the processing and steps to be taken to mitigate the risks.

8. Data Breach

A personal data breach is one which results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Under GDPR, notification to the ICO of a breach which is likely to result in a risk to the rights and freedoms of individuals is mandatory. This would normally represent the loss of extensive records; special category personal data; or children's records.

All such breaches should be notified by the Data Controller to the Information Commissioner's Office within 72 hours of identifying the breach. Responsibility for reporting is delegated to the incumbent/priest in charge, or churchwardens during vacancy.

Breaches not likely to result in a risk to the rights and freedoms of individuals (e.g. deletion of a small number of records, email data incorrectly sent to a trusted individual who was not the intended recipient, failure to BCC individuals in circular emails) should be reported to the PCC Secretary, who will keep a record of the breach and any remedial action undertaken to mitigate the effects of the breach.

9. Policy Review

This policy and its implementation will be reviewed annually and any instances of non-compliance reported to the annual parochial church meeting.