The Benefice of Purley St. Mark and St. Swithun
Data Protection Policy **March 2018** *(rev 2.2)*

1. Introduction:

The General Data Protection Regulations [***GDPR***] require organisations to control how personal data is managed, whether this is electronic or on paper or other materials.

The Benefice of Purley St. Mark and St. Swithun [***BPMS***] takes its responsibilities for data protection very seriously.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

> 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

This policy applies to all staff, committees, groups and organisers [***Approved Users***] working specifically for or with the incumbent of BPMS [***the Data Controller***]. It applies to all data held by the data controller that can be related to identifiable individuals.

2. Lawful Basis:

Under Article 6 of the GDPR data controllers are required to establish a Lawful Basis for processing (holding and maintaining) data. The basis for BPMS to process data is through:

- **Consent**, under which individuals have given clear consent for data to be processed for a specific purpose.

3. Data Held Against Individuals:

Data will be held as follows

- The General Contact database holds non-sensitive personal information;
- The Electoral Roll is a public list that lists all those on the electoral roll of either church;
- The Planned Giving Recorders hold information about planned giving and gift aid;
- The Lettings Officers record details of Hall lessees for administrative purposes;
- Organisations responsible to the PCCs will hold membership information.

4. Purpose of Data Gathering:

The data controller keeps data on individuals:

- For the day-to-day administration of the churches, and their facilities;
- To help us inform members, parishioners and interested parties about our services, events, charitable work and initiatives;
- To maintain membership, giving, stewardship and support;
- To contact individuals or their next of kin;
- To increase our understanding of the churches' demographic makeup.

5. Responsibilities:

The safe and secure storage of data, its accuracy and maintenance is the responsibility of the Data Protection Officer [*the **DPO***].

All individuals who have access to the data are bound by the law and its application by the DPO.

Duties of the DPO:

- Keeping the data controller and PCCs updated on data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies in line with an agreed schedule;
- Arranging data protection training and advice for individuals covered by this policy;
- Handling data protection questions from individuals covered by this policy;
- Dealing with requests from individuals to view data held by the Data Controller;
- Checking and approving any contracts or agreement with third parties that may handle or manage the data covered by this policy;
- Ensuring that all systems and equipment used for storing data meets acceptable security standards;
- Evaluating any third party services proposed for data storage or processing;
- Approving any data protection statements attached to communications such as emails or letters;

Duties of approved users:

- Data must never be stored informally (e.g. on unsecured home computing equipment, mobile telephones etc.);
- Approved users must receive training in the software for which they will be responsible, and, however the data is stored, for its proper management;
- Approved users are expected to take precautions to ensure that data is kept secure, (e.g. using strong passwords, keeping passwords secret, keeping paperwork secure and locked away);
- Data must never be disclosed to unauthorised individuals or organisations;
- Data must be kept current, and out-of-date data deleted unless it is required for historical purposes within the terms of this policy;
- Approved users must seek the assistance of the DPO if not sure about any aspect of data protection.

6. Data Storage:

*(In this section the word **Database** is used to indicate data stored electronically in any format).*

The Contacts database is kept by a third party company under contract to maintain data security. The database is only accessible by the holders of the following posts:

- Incumbent;
- Curate (if appointed);
- Readers (or unordained ministers licensed to the parish);
- DPO;
- Churchwardens;
- Parish secretary;
- Parish treasurers;
- Planned giving recorders;
- Electoral roll officers;
- Lettings officers;
- Managers of organisations;
- Members of PCCs.

Other databases will be held on local computers. Users wil be registered, and the machines will be password controlled and not available to any other individual. Knowledge of the passwords will be restricted to the Lettings Officers, the Assistant Lettings Officers, the Parish Secretary, organisation managers, and the DPO.

Calendar-related (non-financial) lettings information is held in the main Contacts database.

Use and dissemination of data:

- Data from these databases must not be extracted and stored on other electronic or cloud media, printed, or disseminated in any form, without the express permission of the DPO, except between approved users.
- Local versions of databases are not permitted in any circumstances. If data is required for a particular project or activity it must be password controlled, and deleted as soon as possible after the activity is complete.
- Data must be backed up regularly to a secure medium. If Cloud storage is used, this must be protected by password. If data is archived to CD/DVD, or other permanent medium (only by permission of the DPO) it must be kept securely locked away.
- Printed data must be kept securely locked away and out of sight of unapproved individuals. In this context 'data' means any information held against an individual that is subject to the GDPR.

7. Data Maintenance and Access by Individuals:

Under the Consent lawful basis data may only be held under explicit consent of the data subject.

The GDPR provides the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erase;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

BPMS undertakes to ensure that all individuals' [**subjects'**] rights under the Regulations are respected:

- To keep any information about subjects secure and available only to those who need to see it;
- Not to pass on any information to any third party without the subject's express permission (except where legally compelled so to do);
- To allow subjects to know exactly what information is held at any time;
- To delete any data subjects do not want the organisation to hold;
- Never to sell or give data to any organisation;
- To consult subjects personally before extending the information the organisation wants to hold;
- To behave ethically and to act always in both the letter and spirit of the law.

Requests for information, rectification or deletion will be handled as quickly as possible, and always within one month (as required by the regulations).

If the data subject dies information will be preserved for statistical and historical purposes. Next-of-kin will have the right to correct or delete information about their status. Data about the individual that contains errors will be corrected, but not deleted.

8. Children and Vulnerable Adults:

Where the data subject is legally a child, or is a protected vulnerable adult, no personal data will be held without the express permission of the legal guardian. Sensitive personal data will never be held.

9. Data Portability and Profiling:

Individuals may obtain and reuse their personal data for their own purposes. If requested, all data will be supplied to the individual as an open-format document (CSV file). It will not be possible to transfer data directly to a third party.

Profiling (automated processing of personal data to evaluate information about an individual) will not be carried out by BPMS in any circumstances.

10. Responsible Officers:

Holders of positions of responsibility in regard to data protection may be found in the 'BPMS Data Protection Privacy Notice'.