ST MATTHEW'S WESTMINSTER

DATA PROTECTION POLICY

1. POLICY STATEMENT

The PCC recognises and is committed to its responsibilities under the Data Protection Act 2018 which incorporates the European General Data Protection Regulation in relation to its handling of personal data. "Personal data" is information relating to a living individual who can be identified from that information. The PCC may collect, store and process personal data about congregation members, electoral roll members, and other users of the church ("data subjects") in order to carry out the duties and functions of the church and for making contact with those persons in relation to church and parish matters. Under the Data Protection Act anyone handling personal data must comply with the following six principles of good practice by ensuring that data is:

- Processed fairly and lawfully and in a transparent manner in relation to individuals;

- 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;

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- 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;

- 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;

- 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.

The PCC shall be responsible for, and be able to demonstrate, compliance with the principles.

In addition, the PCC needs to ensure that personal data is:

(a) Not transferred to another country without appropriate safeguards being in place.
(b) made available to data subjects and data subjects allowed to access certain rights in relation to their personal data (see section 3 – Individuals' rights)

2. DEFINITIONS

Personal data is information about a living individual which is capable of identifying directly or indirectly that individual e.g. name and address,

A data breach means a breach of security leading to the accidental or lawful unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing is anything done with /to personal data, including storing it.

Data subject is the person about whom data is processed.

Data controller is the person or organisation who determines the how and what of data processing i.e. St Matthew's PCC and the Incumbent (in relation to pastoral information held which is confidential to individual clergy). As the incumbent is a member of the PCC, there is no need for a data sharing agreement between the two.

3. INDIVIUALS' RIGHTS

Under the Act, individuals have the following rights:

1. To be informed
2. To access data
3. To rectify mistakes
4. To have data erased ('to be forgotten')
5. To restrict processing
6. To make data portable
7. To object to processing
8. To object to automated decision-making.

4 .STATUS OF POLICY

The PCC has approved this policy and is responsible for ensuring it is kept up to date. It sets out the rules on data protection which must be complied with by PCC members, parish officers and employees and parish volunteers ("data users") when they obtain, handle, process, transfer and store personal data during the course of carrying out church and parish business.

The PCC will issue relevant privacy notices to the congregation, role holders, volunteers, contractors and employees which will explain how their data is managed and the purpose for which it is held.

Any person who feels that this policy has not been adhered to, whether in respect of their own personal data, or in respect of a third party's, should raise this with the Data Protection Officer, Jane Kennedy.

5 .RESPONSIBILITIES

The PCC is the Data Controller under the Data Protection Act, and is responsible for the implementation of the Act and for ensuring compliance by data users.

The PCC has appointed a Data Protection Officer to handle day to day queries which may arise, and to provide data users with guidance on Data Protection issues to ensure they are aware of their obligations.

All data users are responsible for ensuring that they understand and comply with this policy. Any personal data handled or stored by them in the course of carrying out church and parish business must be done so in accordance with this policy and the six principles of good practice set out in the Data Protection Act. If a data user is unsure of his/her obligations or has any queries at any time it is his/her responsibility to seek further advice from the Data Protection Officer.

6. COLLECTION OF DATA

Data users must:

1.1 Only collect personal data to the extent that it is required for the specific purpose notified to the data subject. Appropriate Privacy notices will be issued to all data subjects for whom data is held. The Privacy notice will be held on the church website.

1.2 Seek the data subject's consent to the processing of their data where consent is the legal basis for collecting such data. This means that persons providing personal data must be clearly informed about:

- The purpose or purposes for which we intend to process their personal data;
- The types of third parties (if any) with which we may share or to whom we will disclose that personal data; and
- The means, if any, with which data subjects can limit our use and disclosure of their personal data (i.e. provision of an opt-out).
- Under the Data Protection Act, children are able to give consent at age 13, which means that consent should come from the child rather than the parent/guardian from age 13 unless there are other reasons why the child does not have the capacity to consent. If you are seeking consent from a child the PCC must have a child-friendly privacy notice in place. If the child is under age 13, parental consent is required.

1.3 Not use data for direct marketing purposes without the express consent of the data subject and the PCC.

1.4 Not collect or process "sensitive" personal data unless this is absolutely necessary and the express written consent of the data subject has been obtained. (*Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, health, sexual life, and criminal offences*).

1.5 Obtain consent if people's names and reasons for the prayer request are recorded and published on the church website or in a parish newsletter. If prayer requests are spoken in church then this is fine, you do not need consent.(*Question 23*, *Section E Frequently asked questions*,*The GDPR: A Basic Guide to Data Processing for Parishes.* Parish Resources, Church of England)

7. DATA SECURITY

All data users are responsible for ensuring that personal data is held securely and is not disclosed or transferred to any unauthorised third parties. This applies to electronic and paper records. Any unauthorised disclosure or processing will be treated as a breach of this policy and dealt with appropriately. Additional care and security measures should be taken in respect of data which is "sensitive" personal data.

Personal data will only be accessed by people who have a need to know and are authorised to use it e.g. PCC officers and churchwardens, clergy, parish administrator, pastoral assistants.

A notice will be displayed on the church noticeboard to indicate that CCTV is in use; this is a requirement under the General Data Protection Regulation. This data could be seen by the police in the case of a criminal act e.g. burglary.

Guidance will be issued on handling personal data to all data users. Data users will be updated about specific security measures that are required by the Data Protection Officer and these will include:

- keeping desks and cupboards containing confidential information securely locked.
- shredding paper documents that are no longer required.
- data users should ensure that their screens/monitors/papers do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Storing data on a central computer system.
- Password protecting as appropriate.

Any data breaches must be identified, recorded by the Data Protection Officer and reported to the Information Commissioner's Office within 72 hours if there is a risk to the indivdual's freedom and rights.

8. DATA RETENTION

Data users must ensure that all personal data is accurate and up to date by checking the accuracy of any personal data at regular intervals. The Church Office should be immediately informed of any changes to information previously provided.

Reasonable steps should be taken to destroy or erase from our systems all data which is no longer required. The Church Office will retain some items of information for longer than others but only as long as deemed necessary taking into account guidance from the Information Commissioner and House of Bishops. The PCC will comply with the retention schedule which was issued by the Church of England as shown in the appendix to this policy.

9. SAFEGUARDING

In safeguarding cases, different rules on the treatment and disclosure of personal data may apply (for example to prevent the risk of harm to a child or vulnerable adult or where a criminal investigation is ongoing). Advice should be sought from the Diocesan Safeguarding Adviser without delay in circumstances where personal data relating to a safeguarding concern needs to be processed/shared.

10. THE RIGHT OF ACCESS TO INFORMATION

The Data Protection Act 2018 provides an individual with the right to access personal data relating to him/her which is held by the PCC/Church Office. This applies to data held electronically and also manual records that are in a relevant filing system. Any individual who wishes to exercise this right should make the request to the Data Protection Officer in writing to the Church Office or email the Data Protection Officer direct : privacy@stmw.org who shall then be responsible for managing and responding to this request in accordance with relevant guidance from the Information Commissioner.

The Church Office will only release information upon receipt of proof of identity. The requested information will be provided within one month of receipt of the request, unless there is sufficient reason for delay.

Certain information (for example confidential information relating to a third party) will not be disclosed without obtaining the third party's consent to disclose the information.

11. TRAINING

All PCC members must attend a briefing on data protection and attendance records must be retained.
All data users as listed above (PCC officers, clergy, pastoral assistants, volunteers and employees) must receive briefing on data protection and follow the data protection guidance and attendance records must be retained of attendance at the briefing.

Signed:

Date:

This Policy was approved by the PCC on 21 November 2018 and will be reviewed on a regular basis.