THE MINSTER CHURCH OF ST CUTHBURGA,

WIMBORNE MINSTER

DATA PROTECTION POLICY

POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we may collect, store and process personal information about those on the electoral roll of, and members of the congregation of, the Minster Church of Saint Cuthburga, members of groups under the aegis *of* the Parochial Church Council of the Minster Church, employees of the Parochial Church Council, and volunteers (among others) and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (**GDPR**) and other regulations. The GDPR imposes restrictions on how we may use that information.

1.3 This policy does not form part of any contract and it may be amended at any time. Any breach of this policy will be taken seriously.

2. STATUS OF THE POLICY

2.1 It sets out the rules of the Parochial Church Council of the Minster Church of St Cuthburga of Wimborne Minster (the **PCC)** on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with one of the Church Wardens.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion.

3.4 **Data controllers** are the people who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the GDPR

3.5 **Data users** include those members whose work involves using personal data. Data users have a duty to protect the information they handle by following the data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to other people or organisations without the data subject's consent, unless there is a legitimate interest in so doing.

5. FAIR AND LAWFUL PROCESSING

5.1 The GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller (the PCC) or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met, and in most cases the data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may be processed only for the specific purposes notified to the data subject or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of, and consent to, the new purpose before any processing occurs. The PCC will not pass personal data to any external organisation, other than unless required by law to do so, or specifically consented to by the data subject.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data will be collected only to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place.

8. ACCURATE DATA

Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

9. TIMELY PROCESSING

Personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from the PCC's records when it is no longer required.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data will be processed in line with data subjects' rights. Unless subject to an exemption under the GDPR, data subjects have the following rights with respect to their personal data: -

- The right to request a copy of their personal data which the PCC holds about them;
- The right to request that the PCC corrects any personal data if it is found to be inaccurate or out of date;
- The right to request their personal data is erased where it is no longer necessary for the PCC to retain such data;
- The right to withdraw their consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable)
- The right, where there is a dispute in relation to the accuracy or processing of their personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable)
- The right to lodge a complaint with the Information Commissioners Office.

11. DATA SECURITY

11.1 The PCC will use its best endeavours to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The GDPR requires the PCC to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

11.4 **Security procedures include**:

(a) **Secure lockable desks and cupboards.** Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(b) **Methods of disposal.** Paper documents will be shredded. Floppy disks, memory sticks and CD-ROMs and similar hardware will be physically destroyed when they are no longer required.

(c) **Equipment.** Data users will ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

(d) **Passwords and encryption.** Passwords will be used and kept confidential; encryption may also be employed when appropriate.

12. DEALING WITH SUBJECT ACCESS REQUESTS

All Subject requests must be forwarded promptly to the church wardens, who will be responsible for ensuring that they are dealt with effectively and efficiently within the statutory timescales

13. PROVIDING INFORMATION OVER THE TELEPHONE

Any data user dealing with telephone enquiries will be careful about disclosing any personal information held by the PCC. In particular, they will:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

14. MONITORING AND REVIEW OF THE POLICY

14.1 This policy will be reviewed annually by the PCC. Recommendations for any amendments should be reported to the Church Wardens.

14.2 The PCC will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.