The Parish of Christchurch

Christchurch Priory – St George at Jumpers – St John at Purewell

DATA PROTECTION POLICY

The Parochial Church Council (PCC) of Christchurch

1. POLICY

The PCC recognises and is committed to its responsibilities under the UK General Data Protection Regulations (UK GDPR) 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 (the "data controller") 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 UK GDPR anyone handling personal data must comply with the following eight principles of good practice by ensuring that data is:

- Processed fairly and lawfully;
- Processed for limited purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose for which it is used;
- Accurate;
- Not kept longer than necessary;
- Processed in line with data subject’s rights;
- Stored safely and securely; and
- Not transferred to people or organisations situated in countries without adequate protection.

2. 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.

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.

3. RESPONSIBILITIES

The PCC is the Data Controller under the UK GDPR, and is responsible for the implementation of the UK GDPR 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 eight principles of good practice set out in the UK GDPR. 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.

4. COLLECTION OF DATA

Data users must:

4.1 Only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

4.2 Seek the data subject's consent to the processing of their 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).

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

4.4 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*).

5. 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.

Data users will be updated about specific security measures that are required by the Data Protection Officer and these may 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.

6. 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 Parish 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 Parish 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.

7. 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 and/or the Diocesan Registry without delay in circumstances where personal data relating to a safeguarding concern needs to be processed/shared.

8. THE RIGHT OF ACCESS TO INFORMATION

The UK GDPR provides an individual with the right to access personal data relating to him/her which is held by the PCC/Parish 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 who shall then be responsible for managing and responding to this request in accordance with relevant guidance from the Information Commissioner.

The PCC will only release information upon receipt of proof of identity. The requested information will be provided within 40 days 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.

9. Document History

This Policy was approved by the PCC on 16 July 2025 and will be reviewed on a regular basis, initially in 2026.