Data Protection Policy

Guildford Diocesan Board of Finance

Responsible Officer	**Data Protection Officer**
Date first approved by Board	25/09/2023
First Review Date	25/09/2025
Date Review approved by Board	
Next review date	

Author	**Data Protection Officer**

Detail of specific reviews and key changes made

Reviewer(s)	Date	Review Actions	Approved by Board

Registered Address: Church House Guildford, 20 Alan Turing Road, Guildford, Surrey, GU2 7YF

T: 01483 790300 **E:** data.protection@cofeguildford.org.uk www.cofeguildford.org.uk

1. INTRODUCTION AND BACKGROUND

1.1 The Guildford Diocesan Board of Finance (the "DBF") is a Data Controller and consequently must process all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the UK General Data Protection Regulations 2016/679 (the "GDPR") and any other data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "Data Protection Rules").

1.2 The DBF will collect, store, use and otherwise process Personal data about the people with whom it interacts, who are Data Subjects. This may include trustees, officers, parishioners, volunteers, clergy, religious organisations, employees, contractors, suppliers and other third parties.

1.3 The DBF processes Personal Data so that it can comply with its statutory obligations and achieve its charitable objects of promoting and assisting the work, objects and purposes of the Church of England through the operation of its parishes and other activities.

1.4 Every Data Subject has rights in relation to how the DBF processes their Personal Data. The DBF is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieving and maintaining the trust and confidence of Data Subjects. Therefore, the DBF will regularly review its procedures to ensure that they are adequate and up to date.

1.5 All trustees, directors, members, officers, clergy, staff and volunteers of the DBF who are involved in the processing of Personal Data held by the DBF have a duty to protect the data that they process and must comply with this Policy. The DBF will take any failure to comply with this Policy or the Data Protection Rules very seriously. Any such failure may result in legal action being taken against the DBF or the individual responsible.

2. THE DATA PROTECTION PRINCIPLES

2.1 The DBF as a Data Controller is required to comply, and to demonstrate compliance, with the six data protection principles set out in the GDPR, which provide that Personal Data must be:

2.1.1 processed, fairly, lawfully and in a transparent manner;

2.1.2 collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;

2.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4 accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

2.1.5 kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and

2.1.6 processed in a way that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational security measures.

2.2 There is also an overarching principle; the Data Controller must be able to demonstrate compliance with the six principles. Accountability is vital.

3. THE DIOCESAN DATA PROTECTION OFFICER AND REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE

3.1 The DBF Trustees/Directors have overall responsibility for compliance with the Data Protection Rules. However, the Data Protection Officer (the "DPO") shall be responsible for ensuring day-to-day compliance with this Policy and with the Data Protection Rules. The DPO will undergo regular training and the DBF will provide the DPO with sufficient resources and support to carry out their responsibilities. The DPO's contact details can be found in paragraph 15 of this Policy.

3.2 The DBF is registered with the Information Commissioner's Office (the "ICO") as a Data Controller as required by law. The DBF will be responsible for paying the ICO and future fees levied on Data Controllers by the Data Protection Rules.

3.3 This Policy applies to all Personal Data processed by the DBF in whatever form (e.g. paper, electronic, film) and regardless of how it is stored (e.g. electronically or in filing cabinets). It also includes information that is in paper form but is intended to be put into electronic form and to any recordings made such as telephone recordings or CCTV.

3.4 Note that this Policy applies solely to the DBF. The Bishop of Guildford is considered a Data Controller in their own right and is therefore obliged to register with the ICO as a standalone entity. In practice, the two Data Controllers work closely together to deliver their respective function and Personal Data is shared between them routinely but governed by the provisions of their respective policies and privacy notices.

4. HOW THE DBF WILL COMPLY AND DEMONSTRATE COMPLIANCE

4.1 This Policy is intended to ensure that any processing of Personal Data is in accordance with the Data Protection Rules and the data protection principles. The DBF will therefore:

4.1.1 ensure that, when personal information is collected (whether direct from an individual or from a third party), the Data Subject is provided with a Privacy Notice and informed of what data is being collected and for what legitimate purposes(s);

4.1.2 be transparent and fair in processing Personal Data;

4.1.3 take steps to ensure the accuracy of data at the point of collection and at regular intervals thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them;

4.1.4 securely dispose of inaccurate or out-of-date data which is no longer required for the purpose(s) it was collected;

4.1.5 share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures;

4.1.6 ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the European Economic Area (the "EEA") (see section 7.4 of this Policy).

4.1.7 ensure that data is processed in line with the Data Subject's rights, which include the right to:

a) request access to Personal Data held about them by the DBF (including, in some cases, having it provided to them in a commonly used and machine- readable format);

b) have inaccurate Personal Data rectified;

c) have the processing of their Personal Data restricted in certain circumstances;

d) have their Personal Data erased in certain specified situations (in essence where the continued processing of it does not comply with Data Protection Rules);

e) prevent the processing of Personal Data for direct-marketing purposes (which includes fundraising);

f) ask the DBF to prevent processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual; and

g) prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e. without human intervention) and which produce significant and legal effects on them;

4.1.8 ensure that all trustees, officers, clergy, religious organisations, volunteers and employees are aware of the DBF's data protection policies and procedures and their own responsibilities in terms of data protection; and

4.1.9 adopt, and keep under review, a data retention schedule which sets out periods for which different categories of Personal Data will be kept.

4.2 Through adherence to this Policy and related data protection policies, and through appropriate record keeping, the DBF will seek to demonstrate compliance with each of the data protection principles.

4.3 In addition, the Data Protection Rules require the Data Controller to carry out a Data Protection Impact Assessment (a "DPIA") prior to undertaking any processing of Personal Data that is "likely to result in a high risk to the rights and freedoms" of individuals. DPIAs will therefore be considered where appropriate in relation to the implementation of any new projects, services or systems which could result in a high privacy risk to individuals (particularly where new technology is being deployed) and should also consider other regulation relevant to data protection, such as Privacy and Electronic Communications Regulations. Please contact the DPO for guidance (see paragraph 15 of the Policy).

5. DATA SECURITY AND RESPONSIBILITIES OF TRUSTEES, OFFICERS, CLERGY, STAFF AND VOLUNTEERS

5.1 The DBF must ensure that appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful processing or damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). In particular, all trustees, officers, clergy, employees and volunteers should ensure that:

5.1.1 the only individuals who have access to Personal Data and are able to process it are those who are authorised to do so;

5.1.2 Personal Data is stored only on the central Diocesan computer system and not on individual PCs, portable electronic devices or removable storage media, unless those devices are compliant with the Diocesan IT Communication and Monitoring Policy;
5.1.3 passwords are kept confidential, are changed regularly and are not shared between individuals;

5.1.4 PCs are locked or logged off and paper documents containing personal data are securely locked away when individuals are away from their desks;

5.1.5 offices, desks and filing cabinets/cupboards are secured if they contain Personal Data of any kind, whether digital or electronic format or on paper;

5.1.6 when destroying Personal Data, paper documents are securely destroyed and electronic data is securely deleted; and

5.1.7 Personal Data removed from an office is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public; using passwords/passcodes; encrypting portable electronic devices wherever possible and storing such devices securely (e.g. not left in the boot of a car overnight).

Further details on the DBF's requirements in relation to IT security are set out in the IT Communication and Monitoring Policy.

5.2 In the event that you become aware that there has been a Data Breach, you must report this immediately to the DPO, following the Data Breach Procedure at

data.protection@cofeguildfordorg.uk,

Further contact details of the DPO can be found in paragraph 15 of this Policy.

6. PRIVACY NOTICE

6.1 When any Personal data is collected from an individual, they must be provided with a Privacy Notice. The Privacy Notice provides information about what, why and how information is processed and is prepared at a Diocesan, not parish, level. Our Privacy Notices are published online at: Data Protection & Policies - Diocese of Guildford (cofeguildford.org.uk)

7. PROCESSING, DISCLOSURE AND SHARING OF INFORMATION

7.1 The DBF processes Personal Data for a number of different purposes, including:

LAWFUL GROUND FOR PROCESSING PERSONAL DATA

- Where we have an individual's consent
- Where it is necessary for the performance of a contract to which an individual is party
- Where it is necessary for compliance with a legal obligation
- Where it is necessary to protect the vital interests of an individual
- Where it is necessary for the performance of a task in the public interest
- Where it is necessary for the purposes of legitimate interests pursued by the DBF or a third party

LAWFUL GROUND FOR PROCESSING OF **SPECIAL CATEGORIES** OF DATA

- Where we have an individual's explicit consent
- Where it is necessary for compliance with a legal obligation
- Where it is necessary to protect the vital interests of an individual
- Where it is carried out in the course of the DBF's legitimate activities as a not-for-profit body with religious aims
- Where information has manifestly been made public
- Where we are establishing, exercising or defending legal claims
- Where the processing is for reasons of substantial public interest
- Where steps are taken to prevent fraud or other dishonest activity
- Where the process is necessary for archiving historical records

8. DISCLOSING PERSONAL DATA

8.1 When receiving telephone or email enquiries, directors, trustees, members, officers, clergy, employees and volunteers should exercise caution before disclosing any Personal Data. The following steps should be followed:

1. ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the requested information;

2. ask the enquirer to put their request in writing so that their identity and entitlement to receive the information can be verified if the information is particularly sensitive and/or you are not confident the person is entitled to the information;

3. if there is any doubt, refer the request to the DPO for assistance (particularly where special categories of Personal Data are involved);

4. when providing information, ensure that Personal Data is securely packaged and sent by the most appropriate means (e.g. password protected email, documentation shared via SharePoint or similar, special delivery, courier or hand delivery) in accordance with Data Protection Rules, the Privacy Statement and this Policy.

8.2 Please remember that parents and guardians are only entitled to access information about their child if the child is unable to act on their own behalf (e.g. because the child is not mature enough to understand their rights) or if the child has given their consent. If you are unsure about whether or not to provide information about a child to a parent or guardian, please speak to the DPO before providing any information. Children from 12 upwards are generally to be considered as being capable of understanding their rights and making decisions regarding their own information. However, consideration of the particular circumstances and of the child's capacity must be taken into account in each instance.

8.3 Please also remember that individuals are only entitled to information about themselves and not any other third party (e.g. family member, companies, other parishioners or members of clergy or staff).

9. DATA PROCESSORS

9.1 The DBF may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g. pension provider, a third party IT provider). In such situations the DBF will share necessary information with the Data Processor, but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

9.2 Personal Data will only be transferred to a third party Data Processor if the DPO is satisfied that the third party has in place adequate policies and procedures to ensure compliance with Data Protection Rules. There should also be a written contract in place between the DBF and the Data Processor, which includes provisions to ensure that the Data Processor complies with the requirements of the Data Protection Rules. To enter into a contract please refer to the DPO.

10. THIRD PARTY REQUESTS

10.1 The DBF may from time to time receive requests from third parties for access to documents containing Personal Data. The DBF may disclose such documents to any third party where it is legally required or permitted to do so. Such third parties may include health professionals, the Police and other law enforcement agencies, the Charity Commission, HMRC, other regulator, immigration authorities, insurers, local authorities (e.g. Trading Standards), courts and tribunals or organisations seeking references.

10.2 Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal Diocesan operations must immediately contact the DPO.

11. TRANSFERS OF PERSONAL DATA OUTSIDE OF THE UK

11.1 Following its withdrawal from the European Union, the UK has fully incorporated the principles, rights and obligations of the GDPR and the DBF may continue to transfer Personal Data outside of the UK but within the European Economic Area without the need for additional safeguards (in most cases).

11.2 The DBF may transfer Personal Data outside of the UK/EEA subject to appropriate safeguards being met, e.g. where there is a legally binding agreement between the DBF and a data processor or where the DBF and a data processor have entered into a contract incorporating standard data protection clauses recognised or issued in accordance with the UK data protection regime (known as Standard Contractual Clauses).

11.3 The DBF may also transfer Personal Data outside of the UK where requested by the Data Subject, on the basis of the Data Subject's informed consent, for example, where a Data Subject requires their marriage record sent to another country.

11.4 The DPO may also authorise transfers where another legal ground in the Data Protection Rules is met.

12. SUBJECT ACCESS REQUESTS

12.1 Any Data Subject may exercise their rights as set out above (e.g. the right of access to the Personal Data which the DBF holds about them, or the right to have Personal Data erased). Any such requests should immediately be referred to the DPO.

12.2 To be valid, a Subject Access Request may be verbal or made in writing (including requests made by email or on social media) and provide enough information to enable the DBF to identify the Data Subject and to comply with the request.

12.3 All Subject Access Requests will be dealt with by the DPO with support from the DBF's retained Data Protection Advisors. Clergy, employees or volunteers who receive a Subject Access Request must forward it to the DPO immediately in order that such requests can be replied to within strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

12.4 No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to provide additional copies of information previously provided. Where the DBF considers a request to be manifestly unfounded, excessive or repetitive, the DBF may lawfully refuse to respond and if so, the DPO will inform the Data Subject of this in writing within the one-month period.

13. FUNDRAISING AND MARKETING

13.1 'Direct marketing' includes all advertising and promotional activities, including promoting the aims and ideals of not-for-profit organisations.

13.2 Any use of Personal Data for marketing (including fundraising) purposes must comply with Data Protection Rules and the Privacy and Electronic Communications Regulations (the "PECR") (and any replacement legislation) which relate to marketing by electronic means.

13.3 Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or fundraising communications must be sent to them.

13.4 The PECR requires that the DBF has the prior consent of recipients in certain circumstances before it sends unsolicited electronic messages for the purpose of fundraising or other marketing activities (e.g. events).

13.5 In the event of any such activity being undertaken, reference will be made to the guidance issued by the Information Commissioner's Office and the principles set out therein will be adhered to.

14. MONITORING AND REVIEW

14.1 This Policy will be reviewed every three years and is subject to change.

15. CONTACTS

15.1 Any queries or complaints regarding data protection generally or this Policy specifically should be addressed to the Diocesan Data Protection Officer who can be contacted by email at data.protection@cofeguildford.org.uk, by telephone on 01483 790 300 or at the following address: Data Protection Officer, Diocese of Guildford, Church House Guildford, 20 Alan Turing Road, Guildford, Surrey, GU2 7YF

15.2 Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

16. OTHER INFORMATION AND GOVERNANCE POLICIES

16.1 This Policy should be read in conjunction with:

- Privacy Notices
- Data Retention Schedule
- Complaints Policy
- IT Communication and Monitoring Policy
- Discipline Policy

17. GLOSSARY

"Data Controller" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with data protection laws including the GDPR and establishing practices and policies in line with them.

"Data Processor" means a person, organisation or body that processes Personal Data on behalf of and on the instruction of the DBF. Data Processors have a duty to protect the information they process by following data protection laws.

"Data Subject" means a living individual about whom the DBF processes Personal Data and who can be identified from the 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 and the information that the DBF holds about them.

"Personal Data" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, the DBF's possession. Personal Data can be factual (such as name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled the individual to be identified) would fall within the definition.

"Processing" means any activity which involves the use of Personal Data. It includes obtaining, recording or holding or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"Special Categories of Personal Data" (previously called sensitive personal data) means 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 sexuality. It also includes genetic or biometric data. Special categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.