Canterbury Diocesan Board of Finance

Data Protection Policy

1. Purpose and Scope

1.1 This policy provides a framework for ensuring that the Canterbury Diocesan Board of Finance (CDBF) meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). The CDBF is a data controller and a data processor under the GDPR.

The UK GDPR and this policy apply to all the CDBF's personal data processing functions, including those performed on personal data connected with ministers, volunteers, employees, suppliers and partners, and any other personal data the organisation processes from any source. This includes data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

1.2 This policy applies to all employees/staff and other interested parties of CDBF such as volunteers, committee members and outsourced suppliers. Any breach of the UK GDPR will be dealt with under CDBF's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.3 Partners and any third parties working with or for CDBF, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

1.4 The CDBF complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes
- adequate, relevant, and limited to what is necessary
- accurate and, where necessary, up to date
- not kept for longer than necessary
- kept safe and secure

1.5 In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

Our staff have access to several policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, including:

- Data Retention Policy
- Information Security Policy
- Good practice guidelines

2. Information covered by Data Protection Legislation

2.1 The UK GDPR definition of 'personal data' includes any information relating to an identified or identifiable natural living person. Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA, providing the anonymisation has not been done in a reversible way.

2.2 Some personal data is more sensitive and is afforded more protection; this is information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric ID data
- Health data
- Sexual life and/or sexual orientation
- Criminal data (convections and offences)

3. Our Commitment

3.1 The CDBF is committed to transparent, lawful, fair and proportionate processing of personal data. This includes all personal data we process about staff, lay and ordained ministers, stakeholders and those who work or interact with us.

3.2 To enhance the effectiveness of our compliance efforts, the CDBF has appointed a Data Protection Officer (DPO) responsible for Subject Access Requests (SARs) and data breaches, and a DPO responsible for policy, document retention and staff training. Both report to the Archbishop's Council through its GDPR Board. The DPOs are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.3 We have established a layered system of Privacy Notices on our website and track and make available any changes.

3.4 The Bishop's Staff Team and Departmental Directors are responsible for developing and encouraging good information handling practices within Canterbury Diocesan Board of Finance.

3.5 Compliance with data protection legislation is the responsibility of all Employees/Staff of Canterbury Diocesan Board of Finance who process personal data. Departmental Directors are expected to have oversight of data processing and Subject Access Requests that take place within their area of responsibility. All staff undertake training on information governance and security and are required to complete data protection training as part of their induction.

3.6 We carefully consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO, taking appropriate action to make data subjects aware if needed.

4. Key Policy Matters

4.1 Data Protection by Design

Each Department must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility. The subsequent DPIA findings must then be submitted to the DPO for review and approval. Where applicable, the Information Systems Programme Manager, as part of the IT system and application design review process, will cooperate with the DPO to assess the impact of any new technology uses on the security of Personal Data.

4.2 Compliance Review

To ensure best practice is used across the organisation and to monitor and update processes on a regular basis, the DPOs will carry out an annual Data Protection compliance review. This will include assessment of:

- Departmental reviews of data audits
- Privacy Notices
- Policy reviews
- Staff training and awareness
- Security protocols
- Data transfers

Any deficiencies will be addressed by the DPOs in conjunction with Departmental Directors within an agreed and reasonable time frame.

4.3 How we collect data

Personal Data should be collected only from the Data Subject unless one of the following applies:

- The nature of the purpose necessitates collection of the Personal Data from other persons or bodies
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing or transfer of the Personal Data

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

4.4 Consent

Personal Data will only be obtained by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Each Diocesan Department shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their Personal Data.

The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid consent.
- Ensuring the request for consent is made in an easily accessible form, using clear and plain language
- Ensuring the consent is freely given
- Documenting the date, method and content of the disclosures made, as well as the validity, and scope of the consents given
- Providing a straightforward method for a Data Subject to withdraw their consent at any time

4.5 Privacy Notice

The CDBF will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their Personal Data.

The CDBF will make a layered Privacy Notice available on the diocesan website, so that it is easy to select the reason that the CDBF processes personal information and what people might expect it to do when people make contact or use one of our services.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller
- the contact details of the Data Protection Officer(s)
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the period for which the personal data will be stored
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, where applicable
- further information necessary to guarantee fair processing

All data collection forms must include a link to the correct 'layer' of the Privacy Notice be approved by the Data Protection Officer.

4.6 Use of Personal Data

The CDBF uses the Personal Data of its contacts for the following broad purposes:

- To enable us to provide a voluntary service for the benefit of the public within the Diocese of Canterbury
- To administer Parish, Deanery, Archdeaconry and Diocesan membership and governance records
- To manage and maintain our records and accounts
- To communicate about events and services

The use of a contact's information should always be considered from their perspective; whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within expectations that a contact's details will be used by the CDBF to communicate all relevant information about the events and services on offer, but not that the CDBF would then provide their details to Third Parties for marketing purposes.

The CDBF will not process Personal Data unless at least one of the following requirements are met:

1. The Data Subject has given consent to the processing of their personal data for one or more specific purposes
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

3. Processing is necessary for compliance with a legal obligation to which the data controller is subject.
4. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
6. Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the DPO before any such processing may commence.

4.7 Controller-processor contracts

The CDBF uses data processors for operations which require specific expertise, including HR services such as payroll. The UK GDPR imposes a legal obligation on controllers and processors to formalise their working relationship, thus the CDBF has written contracts with all processors. Each contract sets out details of the processing, including the subject matters, duration of the processing, nature and purpose, type of personal data involved, categories of data subject and the controller's obligations and rights.

The CDBF keeps a record of all current processor contracts which is updated when processors change, and contracts are reviewed periodically to make sure they remain up to date.

4.8 Special Categories

The CDBF will only process Special Categories of Data where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject
- The processing is necessary for the establishment, exercise or defence of legal claims
- The processing is specifically authorised or required by law
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health

In any situation where Special Categories of Data are to be processed, the basis for the processing will be clearly recorded and the CDBF will adopt additional protection measures.

4.9 Children and Vulnerable Adults

Children are unable to consent to the processing of personal data for diocesan ministry purposes, so consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Should any Diocesan Department foresee an organisational need for obtaining parental consent for ministry involving children, guidance and approval must be obtained from the DPO before any processing of a child's personal data may commence.

4.10 Data Quality

Each Diocesan Department will ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the Diocese to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required
- Restriction, rather than deletion of personal data, insofar as:
    - a law prohibits erasure
    - erasure would impair legitimate interests of the data subject
    - the Data Subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

4.11 Digital Marketing

As a general rule the CDBF will not send promotional or direct marketing material to a Diocesan Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent.

4.12 Data gathered by Unmanned Aircraft Systems (UAS)

Employees of the CDBF may use UAS in limited circumstances, principally when undertaking building inspections of churches and parsonages. The CDBF is aware that if using UAS in a public space, users are potentially collecting personal information which could be used to identify an individual and thus come under the jurisdiction of UK GDPR.

When using UAS, our employees/staff will endeavour to avoid collecting personally identifiable information, which is understood to be:

- where an individual's face is clearly visible
- anything that allows an individual to be identified by other means (visible address numbers, car number plates, unusual clothing)
- distinguishing bodily characteristics of individuals (tattoos, coloured hair)
- anything that can be used to identify a person's profession or place of work

If personally identifiable information about a person is captured, the user will endeavour to inform them about it in line with this policy, referring them to our Privacy Notice and letting them know they have the right to remove data.

During the planning stage of any UAS flight, users should look to minimise the amount of personally identifiable data collected by assessing the layout of the site to identify any houses, cars or people which may need to be anonymised. If the site poses a high risk of people on the ground being identified, a Data Protection Impact Assessment (DPIA) must be carried out.

4.13 Data Retention

To ensure fair processing, personal data will not be retained by the CDBF for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which Diocesan Teams need to retain personal data is in accordance with the Data Retention Policy.

Any personal data processed for the purposes of Safeguarding will be kept in accordance with our legal requirements and our approach to record keeping is consistent with 'Safeguarding Records: Joint Practice Guidance for the Church of England and the Methodist Church', available from the Church of England website.

4.14 How we protect data

The CDBF, through its Departments, will adopt measures to ensure the security of personal data. Physical, technical and organisational security measures include:

- those outlined in the CDBF Information Security Policy
- locating paper files in locked cabinets, with key access limited to authorised staff
- using secure delivery methods if sending personal data through the post
- ensuring that premises are properly protected with alarms

4.15 Data Subject Access Requests

If an individual makes a request relating to their personal data processed by the CDBF, the DPO will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the DPO and upon successful verification of their identity, the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their personal data
- The source(s) of the personal data, if it was not obtained from the data subject.
- The categories of personal data stored for the data subject
- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the personal data or the rationale for determining the storage period
- The use of any automated decision-making, including profiling
- The right of the data subject to:
    - object to processing of their personal data
    - lodge a complaint with the Information Commissioner's Office
    - request rectification or erasure of their personal data
    - request restriction of processing of their personal data

All requests received for access to or rectification of personal data must be directed to the DPO, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the CDBF to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

If the CDBF cannot respond fully to the request within 30 days, the DPO shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- an acknowledgement of receipt of the request
- any information located to date
- details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- an estimated date by which any remaining responses will be provided
- an estimate of any costs to be paid by the Data Subject (e.g., where the request is excessive in nature)
- the name and contact information of the Diocesan individual who the Data Subject should contact for follow up

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

4.16 Data Inventory

The CDBF has conducted an information audit and established a data inventory and data flow process as part of its approach to Data Protection. This inventory captures:

- the business processes that use personal data
- sources of personal data and processing activity
- the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- flow of information including sharing
- all retention and disposal requirements

5. Glossary

Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to them
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processor	A natural or legal person, Public Authority, Agency or other body which processes personal data on behalf of a Data Controller.
Data Subject	The identified or Identifiable natural person to which the data refers
Employee	An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes volunteers, temporary employees and independent contractors
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Special category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

V0.2 September 2024