The Coventry Diocesan Board of Finance

DATA PROTECTION POLICY

1. Introduction

1.1. The Coventry Diocesan Board of Finance (CDBF) needs to keep certain personal information in a safe, responsible and secure manner to carry out its day to day operations, to meet its objectives and to comply with legal obligations. This Data Protection Policy sets out how the Coventry Diocesan Board of Finance (”we”, “our”, “us”, “the Organisation”) handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2. This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

1.3. This Data Protection Policy applies to all Personnel (”you”, “your”). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. If you are an employee, any breach of this Data Protection Policy may result in disciplinary action. If you are a non-employee, any breaches of this Data Protection Policy may result in us terminating your contract with immediate effect.

1.4. This policy does not form part of an employee’s contract of employment and may be amended from time to time. This Data Protection Policy (together with Related Policies) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Director of Operations (Data Protection Officer).

2. Scope

2.1. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Organisation is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR and Data Protection Act 2018. Personal Data breaches also carry the risk of significant civil sanctions for individuals and in some circumstances, can amount to a criminal offence.

2.2. All CDBF staff and volunteers (including Joint Workers) and Officers (e.g. Archdeacons and clergy) who are responsible for Processing Personal Data, or who supervise such Processing undertaken by diocesan officers, trustees and/or volunteers, are responsible for ensuring all Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.3. All staff and volunteers who process personal data must ensure they not only understand but also act in line with this policy. Breach of this policy may result in disciplinary action.

2.4. To meet our responsibilities staff will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is accurate and, where necessary, up to date;
- Review the length of time information is held;
- Ensure it is kept safely;
- Only those employees or volunteers who are authorised to use the data will be able to access it and process it
- Personal data will only be stored on our central computer system or authorised company Cloud systems. When using PCs/smartphones/tablets/iPads etc. staff and volunteers should do this is line with CDBF's Bring Your Own Device (BYOD), Cloud Solutions and Remote Working Policy.
- Whenever possible data should be accessed via the central office network. If data is stored on the device then the device must have a security feature enabled. If equipment is stolen or lost, even if this is a personal device which holds company data, then the individual must inform the IT Systems Manager immediately to enable the remote access to be disabled. A Personal data Breach must also be reported to the Data Protection Officer (Section 11 below).
- Desks and cupboards will be kept locked when not in use if they hold personal data of any kind.
- When destroying personal data, paper documents will be shredded and CD-ROMs will be physically destroyed or disposed of professionally. (The IT Systems Manager should be consulted when destroying any electronic data.) When personal data is not required it should also be deleted from Trash/Deleted Items folders to prevent recovery.
- Data users will be required to ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock their computer when it is left unattended.
- Ensure the rights people have in relation to their personal data can be exercised.

2.5. The Data Protection Officer is responsible for overseeing this Data Protection Policy and developing Related Policies. That post is held by Stephen Davenport, 02476 521346, Stephen.Davenport@Coventry.Anglican.org

2.6. Please contact the Data Protection Officer with any questions about the operation of this Data Protection Policy or the UK GDPR and Data Protection Act 2018 or if you have any concerns that this Data Protection Policy is not being followed. In particular, you must always contact the Data Protection Officer in the following circumstances:

2.6.1. if you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests used by the Organisation) (see Section 5 below);

2.6.2. if you need to rely on Consent and/or need to capture Explicit Consent (see Section 5 below);

2.6.3. if you need to draft Privacy Notices (see Section 5 below);

2.6.4. if you need any assistance dealing with any rights invoked by a Data Subject (see Section 6);

2.6.5. if you are unsure about the retention period for the Personal Data being Processed (see Section 10 below);

2.6.6. if you are unsure about what security or other measures you need to implement to protect Personal Data (see Section 11 below);

2.6.7. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section 11 below).

2.6.8. if there has been a Personal Data Breach (Section 11 below);

2.6.9. if you are unsure on what basis to transfer Personal Data outside the EEA (see Section 11 below);

2.6.10. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Section 12 below) or plan to use Personal Data for purposes others than what it was collected for;

2.6.11. if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section 12 below); or

2.6.12. if you need help complying with applicable law when carrying out direct marketing activities (see Section 13 below).

3. Interpretation

Definitions

3.1. **Automated Decision-Making (ADM):** when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK UK GDPR and Data Protection Act 2018 prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

3.2. **Automated Processing:** any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

3.3. **Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

3.4. **Data Controller:** the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own commercial purposes.

3.5. **Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce high risk data processing activities. DPIA can be carried out as part of Privacy by Design. DPIA's should be conducted for all major system or business change programs involving the Processing of Personal Data and the circumstances detailed in section 12.

3.6. **Data Processor:** includes any person or organisation that Processes Personal Data on behalf of a Data Controller and in accordance with the Data Controller's instructions.

3.7. **Data Protection Lead:** means an individual assigned with the responsibility for overseeing our compliance with UK GDPR and Data Protection Act 2018.

3.8. **Data Protection Officer:** the person required to be appointed in specific circumstances under the UK GDPR and Data Protection Act 2018.

3.9. **Data Retention Policy:** our internal policy which documents the retention periods for Personal Data we hold and the agreed Process for disposal of such Personal Data.

3.10. **Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

3.11. **EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

3.12. **Explicit Consent:** consent which requires a very clear and specific statement (that is, not just action).

3.13. **UK General Data Protection Regulation (UK GDPR):** the UK General Data Protection Regulation. Personal Data is subject to the legal safeguards specified in the UK GDPR.

3.14. **Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Identifiers can include an identification name, location data or online identification or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

3.15. **Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood; deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

3.16. **Personnel:** all employees, workers, contractors, agency workers, consultants, directors and others.

3.17. **Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR and Data Protection Act 2018.

3.18. **Privacy Notices**: separate notices setting out information that may be provided to Data Subjects when the Organisation collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or customer privacy notices which refer to a long privacy policy) or they may be stand alone, one time privacy statements covering Processing related to a specific purpose.

3.19. **Privacy Policy:** the Organisation's privacy policy which provides more detailed information how it Processes Personal Data often cross referred to in a privacy notice and available on the Organisation's website (or if an employee the privacy policy available in the staff handbook).

3.20. **Process, Processing or Processed:** any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

3.21. **Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

3.22. **Related Policies:** the Organisation's policies, operating procedures or processes relating to data protection.

3.23. **Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3.24. **Staff Privacy Policy:** our internal privacy policy which details how we use employees, workers, contractors, agency workers, consultants, directors, members and other related individuals' Personal Data

4. Personal Data Protection Principles

4.1. We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR and Data Protection Act 2018 which require Personal Data to be:

4.1.1. Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency)**.

4.1.2. Collected only for specified, explicit and legitimate purposes **(Purpose Limitation).**

4.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed **(Data Minimisation)**.

4.1.4. Accurate and where necessary kept up to date **(Accuracy)**.

4.1.5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed **(Storage Limitation)**.

4.1.6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage **(Security, Integrity and Confidentiality)**.

4.2. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above **(Accountability)**.

5. Lawfulness, Fairness, Transparency

Lawfulness And Fairness

Basis for processing Personal Data

5.1. Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR and Data Protection Act 2018 restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3. The UK GDPR and Data Protection Act 2018 allows Processing for specific purposes, some of which are set out below:

5.3.1. the Data Subject has given his or her Consent;

5.3.2. the Processing is necessary for the performance of a contract with the Data Subject;

5.3.3. to meet our legal compliance obligations;

5.3.4. to protect the Data Subject's vital interests; or

5.3.5. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests needs to be set out in applicable Privacy Notices.

Sensitive Personal Data

5.4. The Organisation may from time to time need to process Sensitive Personal Data. We will only process Sensitive Personal Data if:

5.4.1. we have a lawful basis for doing so as set out above; and

5.4.2. one of the special conditions for Processing Sensitive Personal Data applies, for example:

5.4.3. the Data Subject has given Explicit Consent;

5.4.4. the Processing is necessary for the purposes of exercising the employment law rights or obligations of the Organisation or the Data Subject;

5.4.5. the Processing is necessary to protect the Data Subject's vital interests, and the Data Subject is physically incapable of giving Consent;

5.4.6. Processing relates to Personal Data which are manifestly made public by the Data Subject;

5.4.7. the Processing is necessary for the establishment, exercise or defence of legal claims; or

5.4.8. the Processing is necessary for reasons of substantial public interest.

5.5. Before processing any Sensitive Personal Data, Personnel must notify the Data Protection Officer of the proposed Processing, so that they can assess whether the Processing complies with the criteria noted above.

5.6. Sensitive Personal Data will not be Processed until:

5.6.1. the assessment referred to in paragraph 5.5 has taken place; and

5.6.2. the individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the Processing, the purposes for which it is being carried out and the legal basis for it.

5.7. In relation to Sensitive Personal Data, the Organisation will comply with the procedures set out in paragraph 5.8 and 5.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

5.8. **During the recruitment process:** the HR department, with guidance from the Data Protection Officer, will ensure that (except where the law permits otherwise):

5.8.1. during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;

5.8.2. if Sensitive Personal Data is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview no record is kept of it and any reference to it is immediately deleted or redacted;

5.8.3. any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

5.8.4. ‘right to work’ checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

5.8.5. we will not ask health questions in connection with recruitment and only ask health questions once an offer of employment has been made.

5.9. **During employment**: the HR department, with guidance from the Data Protection Officer, will process Personal Data and Sensitive Personal Data in accordance with our Staff Privacy Policy.

Consent

5.10. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR and Data Protection Act 2018, which may include Consent.

5.11. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.12. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.13. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for some types of Automated Decision Making and for cross border transfers where we do not rely on adequate safeguards. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

5.14. You will need to evidence Consent captured and keep records of all Consents so that the Organisation can demonstrate compliance with Consent requirements.

Transparency (Notifying Data Subjects)

5.15. The UK GDPR and Data Protection Act 2018 requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.16. Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR and Data Protection Act 2018 including but not limited to the identity of the Data Controller and the Data Protection Officer, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

5.17. When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the UK GDPR and Data Protection Act 2018 as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and Data Protection Act 2018 and on a basis which contemplates our proposed Processing of that Personal Data.

6. Data Subjects Rights and Requests

6.1. Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

6.1.1. to be informed about how, why and on what basis their Personal Data is being processed (Privacy Notice):

6.1.2. withdraw Consent to Processing at any time;

6.1.3. request access to their Personal Data that we hold;

6.1.4. prevent our use of their Personal Data for direct marketing purposes;

6.1.5. ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

6.1.6. restrict Processing in specific circumstances;

6.1.7. challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

6.1.8. request a copy of an agreement under which Personal Data is transferred outside of the EEA;

6.1.9. object to decisions based solely on Automated Processing, including profiling (ADM);

6.1.10. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

6.1.11. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

6.1.12. make a complaint to the supervisory authority (often the Information Commissioner's Office); and

6.1.13. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

6.2. You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation). You must immediately forward any Data Subject request you receive to the Data Protection Officer.

7. Purpose Limitation

7.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary or where an exemption applies e.g. where further Processing is undertaken for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

8. Data Minimisation

8.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2. You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes and that you only Process Personal Data when performing your job duties which require it.

8.3. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Organisation's data retention policy.

9. Accuracy

9.1. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2. You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. In terms of your own Personal Data, you should let the HR team know if the information you have provided to us changes, for example, if you move house or change details of the bank or building society account to which you are paid.

10. Storage Limitation

10.1. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is Processed.

10.2. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3. The Organisation will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. (See the CDBF Data Retention Policy and CDBF Document Retention Tables).

10.4. You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Organisation's Data Retention Policy. This includes requiring third parties to delete such data where applicable.

10.5. You will ensure Data Subjects are informed of the period for which Personal Data is stored and how that period is determined in any applicable Privacy Notice.

11. Security Integrity and Confidentiality

Protecting Personal Data

11.1. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

11.3. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure and you must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

11.4. You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.4.1. Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

11.4.2. Integrity means that Personal Data is accurate and suitable for the purpose for which it is Processed.

11.4.3. Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

11.5. The CDBF will take appropriate technical and organisational security measures to safeguard personal information. It is the IT System's Manager's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party. Deleted data (files and emails) will be stored for a maximum of 25 days before being permanently deleted from the back-up system and therefore will not be recoverable.

11.6. Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action. Any unauthorised disclosure of personal data to a third party by a volunteer or trustee may result in disciplinary action.

11.7. All CDBF employees, line managers and committee secretaries must ensure, when sharing personal data with committee members or volunteers, that the individuals are aware of their responsibility under the Data Protection Act 2018 and GDPR and that they agree to adhere to the 'Remote Working Guidance for Committee Members and Volunteers' (Appendix 1).

11.8. Each department will take reasonable steps to ensure that data is not held for longer than is necessary.

Sharing Personal Data

11.9. We are required to comply with obligations under data protection legislation where we use third parties to process Personal Data on our behalf (including but not limited to IT software providers and HR payroll providers). In these circumstances, such parties will be acting as our Data Processor and data protection legislation requires us to put in place a contract in writing which contains a number of provisions to help safeguard the Personal Data. If you are responsible for the drafting or negotiation of contracts with Data

Processors, you must seek further advice from the Data Protection Officer to ensure the contracts contain all the necessary data protection provisions.

11.10. Where we share Personal Data with third parties for their own use (and they will not be processing data on our behalf) it will often be necessary to enter into a data sharing agreement. We need to ensure that such agreements contain certain provisions such as the third party will only process the Personal Data for specific purposes, to return the Personal Data to us in certain circumstances and have adequate security measures in place.

11.11. In all cases, we may only share the Personal Data we hold provided the sharing complies with the Privacy Notice/Privacy Policy provided to the Data Subject and, if required, the Data Subject's consent has been obtained.

Reporting A Personal Data Breach

11.12. In accordance with UK GDPR and Data Protection Act 2018 we are required to notify Personal Data Breaches to the applicable regulator within 72 hours of becoming aware of the breach where the breach is likely to result in a risk to the rights and freedom of individuals. It will also be necessary to inform the Data Subject when a breach occurs which is likely to be a high risk to the rights and freedom of the Data Subject.

11.13. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11.14. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately notify the Data Protection Officer and follow our data breach protocol. An internal record of any data breach must also be made within our internal breach log. You should preserve all evidence relating to the potential Personal Data Breach.

11.15. Where we act as Data Processor for a third party, we must make the Data Controller aware of the Personal Data Breach as soon as possible.

Transfer Limitation

11.16. The UK GDPR and Data Protection Act 2018 restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR and Data Protection Act 2018 is not undermined. You may only transfer Personal Data outside the EEA if one of the following conditions applies:

11.16.1. the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms, please see the EU website for details of those countries;

11.16.2. appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

11.16.3. the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

11.16.4. the transfer is necessary for one of the other reasons set out in the UK GDPR and Data Protection Act 2018 including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases.

12. Accountability

12.1. The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

12.2. We must have adequate resources and controls in place to ensure and to document UK GDPR and Data Protection Act 2018 compliance including:

12.2.1. appointing a suitably qualified Data Protection Officer (where necessary) where the appointment of a Data Protection Officer is not a legal requirement we must still appoint an individual/individuals with responsibility for overseeing our compliance with UK GDPR and Data Protection Act 2018 such as a Data Protection Lead;

12.2.2. implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

12.2.3. integrating data protection into internal documents including this Data Protection Policy, Related Policies and Privacy Notices;

12.2.4. regularly training Personnel on the UK GDPR and Data Protection Act 2018, this Data Protection Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by Personnel; and

12.2.5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Record Keeping

12.3. The UK GDPR and Data Protection Act 2018 requires us to keep full and accurate records of all our data Processing activities.

12.4. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents.

12.5. We must also keep records of the name and contact details of the Data Controller and the Data Protection Officer, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data transfers outside the EEA and the safeguards put in place to protect the transfer of such Personal Data, the Personal Data's retention period and a description of the security measures in place.

12.6. If we process Sensitive Personal Data and criminal records information, we will also keep written records of:

12.6.1. the relevant purpose for which the Processing takes place, including (where required) why it is necessary for that purpose;

12.6.2. the lawful basis for our Processing; and

12.6.3. whether we retain and erase the Personal Data in accordance with our policy document and, if not, the reasons for not following our policy.

12.7. Our data processing records must always be kept up to date. Please see ICO guidance for further details regarding the information we must record: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/

12.8. We will conduct regular reviews of the Personal Data we Process and update our documentation according. This may include:

12.8.1. carrying out information audits to find out what Personal Data the Organisation holds;

12.8.2. distributing questionnaires and talking to Personnel across the Organisation to get a more complete picture of our Processing activities; and

12.8.3. reviewing our policies, procedures, contract and agreements to address areas such as retention, security and data sharing.

Training And Audit

12.9. We are required to ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.10. You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy By Design And Data Protection Impact Assessment (DPIA)

Privacy by design

12.11. We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

12.12. You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

12.12.1. the state of the art;

12.12.2. the cost of implementation;

12.12.3. the nature, scope, context and purposes of Processing; and

12.12.4. the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

DPIA's

12.13. Data Controllers must also conduct DPIAs in respect to high risk Processing.

12.14. You should conduct a DPIA (and discuss your findings with the Data Protection Officer when implementing major system or business change programs involving the Processing of Personal Data including:

12.14.1. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

12.14.2. Automated Processing including profiling and ADM which have legal or similarly significant effect on Data Subjects;

12.14.3. large scale Processing of Sensitive Data; and

12.14.4. large scale, systematic monitoring of a publicly accessible area.

12.15. A DPIA must include:

12.15.1. a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

12.15.2. an assessment of the necessity and proportionality of the Processing in relation to its purpose;

12.15.3. an assessment of the risk to individuals; and

12.15.4. the risk mitigation measures in place and demonstration of compliance.

See ICO guidance for further information on how to undertake DPIA's (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/)

Automated Processing (Including Profiling) And Automated Decision-Making

12.16. Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

12.16.1. a Data Subject has Explicitly Consented;

12.16.2. the Processing is authorised by law; or

12.16.3. the Processing is necessary for the performance of or entering into a contract.

12.17. If certain types of Sensitive Data are being Processed, then grounds 12.16.2 or 12.16.3 will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

12.18. If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object.

12.19. We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

12.20. A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken which have a legal effect or similar significant effect on the Data Subject. Note that not all Authorised Processing will have a legal or similar effect on a Data Subject, for example, targeted advertising is generally not considered to have a significant effect on individuals.

13. Direct Marketing

13.1. We are subject to certain rules and privacy laws when marketing to our customers.

13.2. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

13.3. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

13.4. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

14. Changes to this Data Protection Policy

14.1. We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy in June 2025.

14.2. This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Organisation operates.

15. Procedure for requesting information

15.1. Requests should be made in writing and submitted to the Data Protection Officer.

16. Policy review

16.1. This policy will be updated as necessary to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

16.2. In case of any queries or questions in relation to this policy please contact the Data Protection Officer whose details are as follows:

Stephen Davenport
Director of Operations
Stephen.davenport@Coventry.Anglican.org
02476 521346

16.3. This policy will be reviewed at intervals of 2 years to ensure it remains up to date and compliant with the law.

Stephen Davenport

6th June 2025

Appendix 1

Remote Working Guidance for Committee Members and Volunteers

This guidance applies to all volunteers who receive information/data within the scope of Diocesan activity. This includes all volunteers (i.e. Committee members, Associate DDO's, members of the Diocesan Safeguarding Scrutiny group) who work remotely from the Diocesan office. It also applies to third parties working on behalf of the Diocese.

Remote working presents significant risks for the CDBF. Volunteers may have access to information and personal data which is outside the security protections available on the internal CDBF systems or the network protections provided by firewalls and access controls, therefore there are greater risks of unauthorised access to information and loss or destruction of data. To ensure that all staff processing information remotely do so securely and in accordance with the UK GDPR and Data Protection Act 2018, the CDBF has developed this guidance.

All CDBF employees, line managers and committee secretaries must ensure, when sharing personal data with committee members or volunteers, that the individuals are aware of their responsibility under the Data Protection Act and that they agree to adhere to this guidance.

This guidance: -

- is intended for all volunteers who work away from the Diocesan office on an occasional or regular basis.
- applies to anyone undertaking any Diocesan work away from the Diocesan office.
- applies to recorded information in all formats: paper, electronic data, correspondence, and e-mail.

Do:

- Remember that all work-related documents are CDBF records, and as such fall within the scope of Data Protection.
- Make use of security features such as password protection & data encryption.
- Take all reasonable steps to maintain security of and prevent loss or damage to any data and/or records received from or taken away from the CDBF.
- Use your CDBF e-mail account for Diocesan work and your personal email account for personal use only; avoid mixing the two.
- Encrypt memory sticks that hold CDBF information.
- Keep your computer system and applications virus-protected and up to date.
- Reduce the risk of inadvertently breaching the Data Protection Act by ensuring that all data subject to the Act which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).
- Delete all CDBF files from your system when the task is completed and they are no longer required (also delete from your Trash folder).

Do Not:

- Use your home computer to store CDBF information unless authorised.
- Leave paper or electronic files where they could be accidentally viewed by others, including family members.
- Use a personal e-mail account for CDBF business.
- Leave CDBF data or electronic media in unattended vehicles, even if locked in the boot.