Testwood Baptist Church

DATA PROTECTION POLICY

ISSUE 2.1

KATRINA ELKINS

CONTENTS

1 Aims of this policy

1.1 Testwood Baptist Church needs to keep certain information on its members, employees, volunteers, service users and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

1.2 The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) which came into force in the UK on 25th May 2018.

1.3 The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

2 Scope of this policy

2.1 The definition of personal data in data protection law is information that relates to an identifiable living individual.

2.2 This can be information held in electronic format or certain kinds of paper records or manual filing system. Personal data held in electronic records includes:

- Information held on a computer, portable hard drive or USB stick or sent in an email;
- Information held on a phone such as a text message or voicemail;
- Visual images where an individual could be identified which may be held on mobile phones, computers or CCTV recording equipment.

This also covers personal data held within manual filing systems which may be arranged in some kind of order, e.g. chronological or alphabetical, enabling an individual's personal data to be accessible.

2.3 The processing of special categories of personal data called 'sensitive personal data' is permitted only under certain conditions. Article 9 of the GDPR defines this as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sex life or sexual orientation." As a religious body, the processing carried out by Testwood Baptist Church will inevitably relate to an individual's religious beliefs, and is therefore subject to these conditions. Processing of such information is restricted to members or former members of Testwood Baptist Church or to those who have regular contact with the church; and on condition that such data is not disclosed outside of this church without the subject's consent.

2.4 This policy covers personal data handled by employed staff, trustees and volunteers.

3 Responsibilities

3.1 In Testwood Baptist Church overall responsibility for personal data rests with the trustees. On behalf of Testwood Baptist Church, the trustees are responsible for:

- understanding and communicating obligations under the Data Protection Act 2018;
- identifying potential problem areas or risks;
- producing clear and effective procedures;
- registering with the Information Commissioner, and payment of the annual fee.

3.2 All employees, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

3.3 Breach of this policy by an employee may result in disciplinary proceedings. Breach of this policy by a volunteer or trustee may result in termination of their volunteer or trustee role. Where an individual is found to have breached this policy intentionally, recklessly or for personal benefit, they may be liable to prosecution.

3.4 The trustees are accountable for compliance of this policy.

3.5 The Data Protection Trustee is responsible for advising Testwood Baptist Church, and its staff and members, of their legal obligations under data protection law, monitoring compliance of this policy and dealing with any data breaches. Any concerns should be referred to them at

4 The lawful bases for holding personal data

4.1 Before collecting personal information, a lawful basis for processing the data must be identified and documented. There are 6 lawful bases listed in Article 6 of the GDPR:

- **Contract** – this applies where data is necessary to process a contract (e.g. employment);
- **Legal Obligation** – this applies where data is necessary to comply with the law or statutory obligations (e.g. DBS checks for safeguarding);
- **Vital Interests** – where processing of data is necessary to protect someone's life, and where they are incapable of giving consent;
- **Public Interests** (only applies to public bodies)
- **Legitimate Interests** – this applies where the data is necessary for the running of the organisation, and for purposes which an individual would reasonably expect their data to be used. It would have a minimal privacy impact and there would be compelling justification for the processing.
- **Consent** – if none of the other legal conditions apply, then data processing will only be lawful if the individual gives their explicit consent.

4.2 For most purposes at Testwood Baptist Church, the lawful basis will be legitimate interest; in these circumstances, it would be difficult or impossible to provide the services to users without collecting their personal data (such as contact details). This will be the lawful basis used for processing:

- Membership records
- Rotas for ministries
- Attendance records for courses or events
- Provision of pastoral support
- Hire of rooms and resources
- Financial records
- Minutes of church meetings
- Communications records
- Contact details, dates of birth and medical information required for children's activities to enable them to take part and keep them safe

4.3 In relation to contracts, we will collect personal data to manage our employees and to comply with employment law.

4.4 We will collect personal data to fulfil our legal obligations. This includes keeping financial records which are required by HMRC; and carrying out health and criminal record checks for employees and volunteers.

4.5 In other circumstances, the consent of the individual will be obtained. This will be done primarily by using 'ChurchSuite' where individual users exercise control of their own personal data. This allows them to choose whether or not they wish to receive general information from Testwood Baptist Church. Church members may also choose which parts of their personal data, if any, they wish to share with other members.

4.6 Where consent is used as the lawful basis, we will ask for consent to be given for specific ('granular') purposes and only when a real choice exists. We will ensure that information we give is clear and unambiguous, and that consent is freely given. We will inform people that they may withdraw their consent at any time and explain how to do this.

4.7 We will keep a record of those who have given their consent, the date of consent and the purposes for which we may use their personal information.

5 Collecting and processing personal data

5.1 Before collecting personal data, we will consider what information is necessary for our purposes and will not collect more than is needed. This is to ensure we comply with the requirement to collect only that which is adequate, relevant and not excessive.

5.2 Where appropriate we will carry out Data Protection Impact Assessments (DPIAs) in order to ensure the personal data we collect is justified, necessary and proportionate. A record of DPIAs will be kept on file.

5.3 At the time of collecting the personal data, we will inform data subjects of the lawful basis for collection, why the information is being collected, what the information will be used for, and who will have access to it. The Testwood Baptist Church Privacy Notice can be accessed on the church website (www.testwoodbaptist.org/privacy) and on MyChurchSuite where users have chosen to use this. Paper copies are also available from the Reception desk.

5.4 We will only process data for the specific purposes explained in our privacy notices or for other purposes permitted by law.

5.5 We will give information in a way that is concise, transparent, intelligible and easily accessible, written in clear and plain language, and is free of charge.

5.6 We will ensure personal information is up to date and accurate by reminding people to update their details at least annually.

5.7 We will ensure that sensitive personal data is only used for the exact purpose for which permission was given.

5.8 We will keep a record of data processing activities as required by the law.

6 Storage and disposal of personal data

6.1 Paper records will be kept in a locked filing cabinet within the church offices, which are locked when not in use.

6.2 Electronic records may be held within ChurchSuite; or on password protected computers. Data will also usually be held on a server located within a church office.

6.3 We will keep personal data records only for as long as necessary to facilitate the purpose for which it was obtained; or to fulfil our legitimate interests; or for as long as is required by the law.

6.4 We will delete or dispose of personal data safely when it is no longer required.

6.5 We will ensure the rights people have in relation to their personal data can be exercised.

7 Security of Personal Data

7.1 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

7.2 We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing. Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following:

a) the quality of the security measure;
b) the costs of implementation;
c) the nature, scope, context and purpose of processing;
d) the risk to the rights and freedoms of data subjects;
e) the risk which could result from a data breach.

7.3 Measures may include:

a) technical systems security;
b) measures to restrict or minimise access to data;
c) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
d) physical security of information and of our premises;
e) organisational measures, including policies, procedures, training and audits;
f) regular testing and evaluating of the effectiveness of security measures.

7.4 Only staff and volunteers who have been authorised by the Trustees will be able to access personal information.

7.5 Staff computers shall be password-protected. Staff must ensure they log off at the end of each session and must not allow others to use their login. Passwords should never be shared with others. Sharing a password is a data breach, which may result in disciplinary action.

7.6 Extra vigilance will be used when sending emails. Where possible, emails should be sent from a Testwood Baptist email account or from ChurchSuite. The sender should check carefully to ensure the recipient is the person intended. When sending an email to multiple recipients, we will BCC the email addresses to protect their privacy. We will try to avoid sending sensitive personal information by email.

8 Sharing Data

8.1 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply. Only authorised and properly instructed staff and trustees are allowed to share personal data.

8.2 We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO's statutory *Data Sharing Code of Practice* when sharing personal data with other data controllers. Legal advice will be sought as required.

9 The Rights of Individuals

9.1 We will process personal data in line with data subjects' rights. The GDPR provides the following rights for individuals:

- The right to be informed of how their data will be used;
- The right to access their data;
- The right to rectification if data is found to be incorrect;
- The right to erasure of data when no longer required (subject to circumstances);
- The right to restrict processing (in certain circumstances);
- The right to data portability;
- The right to object to the processing of their personal data in certain circumstances, including direct marketing;
- The right not to be subject to automated decision making and profiling.

9.2 In order to comply with the GDPR, Testwood Baptist Church upholds these rights. Anyone whose personal information we process has the right to:

- Be informed about what their information will be used for;
- Know what information we hold about them;
- Know how to gain access to this information;
- Know how to keep it up to date;
- Prevent processing of their personal data in some circumstances;
- Have inaccurate data amended;
- Have their personal data erased when it is no longer necessary for the purpose for which it was collected;
- Obtain and reuse their data for their own purposes;
- Withdraw their consent where we are relying on consent as the lawful basis;
- Have access to our Data Protection policy.

10 Subject Access Requests

10.1 If an individual wishes to access their personal data, or to have their personal data rectified where it is inaccurate, he/she should apply in writing or electronically to the Operations Manager.

10.2 The following information will be required before access is granted:

- Name, address and telephone number of the person making the request
- Their relationship with Testwood Baptist Church
- Dates/timescales to be covered by the request

- Proof of identity, e.g. passport, birth certificate.

10.3 A copy of the personal data we hold will be provided free of charge. (A charge may be made to cover administrative costs only where the request is deemed to be excessive.

10.4 We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one month of receiving the request. If the request is complex, this may be extended to 2 months and the person who made the request will be informed of the reason for this.

11 Direct Marketing

11.1 Direct Marketing refers to any contact made by organisations to individuals for the purposes of promoting the organisation's aims. At Testwood Baptist Church, we will comply with the GDPR and the Privacy and Electronic Communications Regulations (PECR) with regard to direct marketing. This includes contacting data subjects by post, email, text message, social media messaging and telephone.

11.2 Any direct marketing communication will identify Testwood Baptist Church as the sender and will explain how the recipient can exercise their right to object to receiving any similar communication in the future.

11.3 We will obtain consent to contact people by email, phone or text, with general news and information about church services and events. If a data subject withdraws their consent, we will stop sending them such information.

12 Training

12.1 The law requires that those handling personal data are trained to do so. We will provide training and awareness-raising about the Data Protection laws and how it is followed in this organisation. We will keep a record of training provided and attended.

12.2 We will ensure that everyone managing and handling personal information is aware of our policies and procedures and that any disclosure of personal data is in line with our procedures.

12.3 On induction an employee, trustee or volunteer will be given this policy and other relevant policies to read and sign; he/she will also be given other relevant information regarding, e.g. the importance of using passwords on computers, keeping files and offices locked.

12.4 We will provide general training at least annually for all staff to raise awareness of their obligations and our responsibilities, as well as to outline the law.

13 Data Breaches

13.1 Where staff or volunteers think this policy may not have been followed, or data might have been breached or lost, this will be reported immediately to the Data Protection Trustee.

13.2 We will keep a record of all data breaches, even if they are not reported to the ICO.

13.3 Where a data breach is likely to result in any risk to a person, we will report the breach to the ICO within 72 hours of becoming aware of the breach, as required by law. Where a breach might result in high risk to a person, we will also inform the data subject.

14 Monitoring and Review

14.1 This policy will be reviewed annually to ensure it remains up to date and compliant with the law.

This policy was agreed by the trustees on 16th July 2018.

Review is due July 2019.