Tillicoultry Baptist Church

DATA PROTECTION POLICY

Adopted: May 5, 2018

Tillicoultry Baptist Church is committed to protecting all information that we handle about people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

Contents

Section A – What this policy is for

1. Policy statement

1.1 Tillicoultry Baptist Church is committed to protecting personal data and respecting the rights of our **data subjects**; the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all current legislation including General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations 2003 (PECR) and the Data Protection Act 2018 and adopting good practice.

We process personal data to help us:

a) maintain our list of church members and regular attenders;

b) provide pastoral support for members and others connected with our church;

c) provide services to the community including Café 2:16, Youth Group, Mother & Toddler groups, Events for Seniors, special events at Easter and Christmas, Holiday Clubs, Gala Day, …

d) safeguard children, young people and adults at risk;

e) recruit, support and manage staff and volunteers;

f) maintain our accounts and records;

g) promote our services;

h) maintain the security of property and premises;

i) respond effectively to enquirers and handle any complaints

1.2 This policy has been approved by the church's Charity Trustees who are accountable for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

2. Why this policy is important

2.1 We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

2.2 This policy sets out the measures we are committed to taking as an organisation and, what the Trustees will do to ensure we comply with the relevant legislation.

2.3 In particular, and in compliance with GDPR principles, we will make sure that all personal data is:

a) processed **lawfully, fairly and in a transparent manner**;

b) collected and processed for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;

c) **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed;

d) **accurate** and, where necessary, up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a **secure** manner, by using appropriate technical and organisational means;

These are further explained at paragraphs 8-13

3. How this policy applies to you & what you need to know

3.1 **As an employee, trustee or volunteer** processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy it is important that you contact our Data Protection Lead immediately so that we can take swift action to try and mitigate the impact of the breach.

3.2 **As a Trustee/Ministry Leader:** You are required to make sure that when processing data in your Ministry area, you and those in your team, comply with this Data Protection Policy.

3.3 **As a data subject of Tillicoultry Baptist Church:** We will process your personal information in accordance with this policy.

3.4 **As an appointed data processor/contractor:** Companies who might be appointed by us as a data processor are required to comply with this policy and in accordance with the terms of the contract. Any breach will be taken seriously and could lead to us taking contract enforcement action against the company, or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the Data Controller (Trustees) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

3.5 **Our Data Protection Lead** is responsible for advising Tillicoultry Baptist Church and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at data@tillicoultrybaptist.org.

3.6 Before you collect or process any personal data as part of your ministry/service for Tillicoultry Baptist Church, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data. Please refer to Section 4 below as regards training requirements.

3.7 All our processing and responses to data protection matters will be in line with this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Data Protection Lead.

4. Training and guidance

4.1 We will provide general training at least annually for all Volunteers/Ministry Leaders/Trustees to raise awareness of their obligations and our responsibilities, as well as to outline the law.

4.2 We may also issue procedures, guidance or instructions from time to time. Ministry Leaders/Trustees must set aside time for their team to look together at the implications for their work.

Section B – Our data protection responsibilities

5. What personal information do we process?

5.1 In the course of our ministry/service, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers.

5.2 We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, and visual images of people.

5.3 In some cases, we hold types of information that are called **"special categories"** of data in the GDPR. This personal data can only be processed under strict conditions.

> **'Special categories' of data** (as referred to in the GDPR) includes information about a person's: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

5.4 We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is an overarching safeguarding requirement to process this data for the protection of children and adults who may be put at risk in our church.

6. Making sure processing is fair and lawful

6.1 Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

6.2 Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

a) the processing is **necessary for a contract** with the data subject;

b) the processing is **necessary for us to comply with a legal obligation**;

c) the processing is necessary to protect someone's life (this is called "**vital interests**");

d) 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 controller

e) the processing is **necessary for the legitimate interests** pursued by Tillicoultry Baptist Church or another organisation, unless these are overridden by the interests, or fundamental rights and freedoms of the data subject.

f) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear **consent**.

How can we legally use 'special categories' of data?

6.3 Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

a) the processing is necessary for **carrying out our obligations under employment and social security and social protection law**;

b) the processing is necessary to **protect the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;

c) the processing is carried out in the **course of our legitimate activities** and only relates to our members, former members or persons we are in regular contact with in connection with our purposes;

d) the processing relates to personal data which is manifestly made public by the data subject;

e) the processing is necessary for **pursuing or defending legal claims**.

f) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit consent**.

6.4 Before deciding which condition should be relied upon, we may refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

What must we tell individuals before we use their data?

6.5 If personal data is collected directly from the individual, we will inform them about: our identity/contact details and those of the Data Protection Lead; the purposes for processing, and its legal basis; if relying on legitimate interests what those interests are; who we will share the data with; whether we intend to send the data outside of the European Union; how long the data will be stored; and the data subjects' rights.

This information is referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

6.6 If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described in paragraph 6.55 as well as: the categories of the data concerned; and the source of the data.

This information will be provided to the individual in writing and no later than within **1 month** after we receive the data, unless a legal exemption applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

7. When we need consent to process data

7.1 Where none of the other lawful bases apply to the processing we will obtain consent from the data subject. We will clearly separate out what processes require consent, and detail the purposes for which we are collecting the data and how we intend to use it. Consent will be specific to each process and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

7.2 Consent can however be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

8. Processing for specified, explicit and legitimate purposes

8.1 We will only process personal data for the specified, explicit and legitimate purposes explained in our privacy notices (as described above in paragraph 6.5.5) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described at paragraph 6, unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and limited

9.1 We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data "just in case" we want to process it later.

10. Accurate data

10.1 We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

11. Keeping data and destroying it

11.1 We will not keep personal data longer than is necessary for the purposes for which it was collected. We will comply with both legal obligation and official guidance issued to organisations like ourselves about retention periods for specific records.

11.2 Information about how long we will keep records can be found in our Data Retention Schedule.

12. Security of personal data

12.1 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.

12.2 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, and anything else that is relevant:

a) the quality of the security measure;

b) the costs of implementation;

c) the nature, scope, context and purpose of processing;

d) the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;

e) the risk which could result from a data breach.

12.3 Measures may include:

a) technical systems security;

b) measures to restrict or minimise access to data;

c) pseudonymisation as appropriate

d) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;

e) physical security of information and of our premises;

f) organisational measures, including policies, procedures, training and audits;

g) regular testing and evaluating of the effectiveness of security measures.

13. Keeping records of our data processing

13.1 To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

Section C – Working with people we process data about (data subjects)

14. Data subjects' rights

14.1 We will process personal data in line with data subjects' rights as set out in the GDPR, including the right to:

a) request access to any of their personal data held by us (known as a Subject Access Request);

b) request to have personal data concerning him or her erased without undue delay in terms of article 17 of the GDPR

c) ask to have inaccurate personal data rectified;

d) restrict processing, in certain circumstances;

e) object to processing, in certain circumstances, including preventing the use of their data for direct marketing;

f) data portability, which in certain circumstances means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

g) not be subject to automated decisions, in certain circumstances; and

h) withdraw consent when we are relying on consent to process their data.

14.2 If a Volunteer/Ministry Leader/Trustee receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Lead **immediately**.

14.3 We will act on all valid requests as soon as possible and at the latest within **one calendar month**, unless we have reason to, and can lawfully, extend the timescale. This can be extended by up to two months in some circumstances.

14.4 All data subjects' rights are provided free of charge.

14.5 Any information provided to data subjects will be concise and transparent, using clear and plain language.

15. Direct marketing

15.1 We will comply with the GDPR, PECR and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

> **Direct marketing** means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

15.2 Any direct marketing material that we send will identify Tillicoultry Baptist Church as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

Section D – working with other organisations & transferring data

16. Sharing information with other organisations

16.1 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 we are legally obliged to share the information or other legal exemptions apply to informing data subjects about the sharing. Only authorised and properly trained Volunteers/Ministry Leaders/Trustees are allowed to share personal data.

16.2 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*** (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

17. Data processors

17.1 Before appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

17.2 We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

18. Transferring personal data outside the European Union (EU)

18.1 Personal data cannot be transferred (or stored) outside of the European Union unless this is compliant by the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU.

18.2 We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR

Section E – Managing change & risks

19. Data protection impact assessments

19.1 When we are planning to carry out any data processing which is likely to result in a high risk to the rights and freedoms of data subjects, we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

19.2 We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO before processing any data.

19.3 DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

20. Dealing with data protection breaches

20.1 Volunteers/Ministry Leaders/Trustees, think that this policy has not been followed, or data might have been inappropriately processed or shared, or lost, this must be reported **immediately** to the Data Protection Lead.

20.2 All Data Processors are obliged, in terms of their contract, to report any data breaches.

20.3 We will keep records of personal data breaches, even if we do not report them to the ICO.

20.4 We will report all data breaches which are likely to result in a risk to the rights and freedoms of any data subject, to the ICO. Reports will be made to the ICO within **72 hours** from when the Data Protection Lead becomes aware of the breach and has contacted.

20.5 In situations where a personal data breach causes a high risk to the rights and freedoms of any data subject, we will (as well as reporting the breach to the ICO), inform those data subjects whose information is affected without undue delay.

This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means and the purposes for processing personal data. For Tillicoultry Baptist Church the Trustees are the data controllers.

The data controller is accountable for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data Protection Lead means a designated trustee responsible for advising Tillicoultry Baptist Church and its Volunteers/Ministry Leaders/Trustees about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Details for contacting the Data Protection Lead are included in current Privacy Notices.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us.

Data subjects include <u>all</u> identified or identifiable living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

a) the people we care for and support;
b) our employees (and former employees);
c) consultants/individuals who are our contractors or employees working for them;
d) volunteers;
e) tenants;
f) trustees;
g) complainants;
h) supporters;
i) enquirers;
j) advisers and representatives of other organisations.
k) members

ICO means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.
Scotland Information Commissioner's Office • 45 Melville Street • Edinburgh • EH3 7HL
Tel: 0303 123 1115

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable whether directly or indirectly. A natural person must be an individual and cannot be a company or a public body.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion expressed by or about that person, or their actions and behaviour which is capable of identifying them.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the 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 can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special categories of data (as identified in the GDPR) includes information about a person's:

a) Racial or ethnic origin;

b) Political opinions;

c) Religious or similar (e.g. philosophical) beliefs;

d) Trade union membership;

e) Health (including physical and mental health, and the provision of health care services);

f) Genetic data;

g) Biometric data;

h) Sexual life and sexual orientation.