

# **FOLKESTONE BAPTIST CHURCH**

## **DATA PROTECTION POLICY FOR HILL ROAD AND CAPEL**

**This policy was first adopted by the Church's Charity Trustees on 9<sup>th</sup> May 2018 under the General Data Protection Regulations (GDPR) introduced on 25<sup>th</sup> May 2018. The policy was subsequently reviewed in line with Baptist Union guidelines and the revised policy document was approved by the Charity Trustees on 9<sup>th</sup> June 2021.**

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

## Contents

<u>Section A – What this policy is for</u>	Page
1. Policy Statement .....	3
2. Why this policy is important .....	3
3. How this policy applies to you and what you need to know .....	4
4. Training and guidance .....	5
<u>Section B – Our data protection responsibilities</u>	
5. What personal information do we process? .....	5
6. Making sure processing is fair and lawful .....	6
7. When we need consent to process data .....	8
8. Processing for specified purposes .....	8
9. Data will be adequate, relevant and not excessive .....	8
10. Accurate data .....	8
11. Keeping data and destroying it .....	8
12. Security of personal data .....	8
13. Keeping records of our data processing .....	9
<u>Section C – Working with people we process data about (data subjects)</u>	
14. Data subjects' rights .....	9
15. Direct Marketing .....	10
<u>Section D – Working with other organisations and transferring data</u>	
16. Sharing information with other organisations .....	10
17. Data Processors .....	11
18. Transferring personal data outside the United Kingdom (UK) .....	11
<u>Section E – Managing change and risks</u>	
19. Data Protection Impact Assessments .....	11
20. Dealing with Data Protection breaches .....	12
<u>Schedule 1: Definitions and useful terms .....</u>	13
<u>Schedule 2: ICO Registration .....</u>	15
<u>Schedule 3: Appropriate Policy Document .....</u>	16

## **Section A – What this policy is for**

### **1. Policy Statement**

- 1.1. **Folkestone Baptist Church (FBC)** is committed to protecting **Personal Data** and respecting the rights of our **Data Subjects**, i.e. 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 relevant laws and adopting good practice.

We process **Personal Data** to help us:

- (a) maintain our list of church members and regular worshippers;
  - (b) provide pastoral support for members and others connected with our church;
  - (c) provide services to our community;
  - (d) safeguard children, young people and adults at risk;
  - (e) recruit, support and manage staff and volunteers;
  - (f) undertake research;
  - (g) maintain our accounts and records;
  - (h) promote our activities and services;
  - (i) maintain the security of property and premises;
  - (j) respond effectively to enquirers and handle any complaints, and
  - (k) for any other reasonable purpose.
- 1.2 This policy has been approved by the Church's Charity Trustees who are responsible 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, 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 each of us will do to ensure we comply with the relevant legislation.
- 2.3. In particular, we will make sure that all **Personal Data** is:
- (a) processed **lawfully, fairly and in a transparent manner**;
  - (b) processed for **specified, explicit and legitimate purposes** and not 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) **not kept longer than necessary** for the purposes for which it is being processed;
- (f) processed in a **secure manner**, by using appropriate technical and organisational means;
- (g) processed in keeping with the **rights of Data Subjects** regarding their **Personal Data**.

### 3. **How this policy applies to you and what you need to know**

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

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for any personal benefit, they may also be liable to prosecution or to regulatory action.

- 3.2 **If you are a leader/manager** you are required to make sure that any procedures that involve personal data you are responsible for in your area of activity follow the rules set out in this Data Protection Policy.
- 3.3 **If you are a Data Subject of FBC** we will handle your personal information in line with this policy.
- 3.4 **If you are an appointed Data Processor/contractor (individual or company)** appointed by us as a **Data Processor** you are required to comply with this policy under the contract with us. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the individual or company, or terminating the contract. **Data Processors** have direct obligations under the UK GDPR, primarily to only process data on instructions from the **Data Controller** and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.
- 3.5. **Our Data Protection Team** are responsible for advising FBC 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.

- 3.6 Before you collect or handle any **Personal Data** as part of your work (paid or otherwise) for FBC 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.
- 3.7 Our procedures will be in line with the requirements of 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 a member of the Data Protection Team.

#### 4. **Training and guidance**

- 4.1 We will provide general training regularly for all staff 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. Managers /leaders 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 work, 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, when 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, employment or medical 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 UK GDPR.

<p>'<b>Special categories</b>' of data (as referred to in the UK 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.</p>
---

**Special category Personal Data** does not include **Personal Data** about criminal allegations, proceedings or convictions, as separate rules apply. Other than in the circumstances described in paragraphs 5.4 to 5.8 below, information relating to criminal convictions and offences should not be processed unless the processing is authorised by law or is carried out under the control of official authority. Special category **Personal Data** can only be processed under strict conditions, including the **Data Subject's** explicit consent (although other alternative conditions can apply in limited, very specific circumstances as described below).

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data.

- 5.4 We may process information relating to criminal proceedings or offences or allegations of offences to safeguard against any risks posed to others under Article 6(1)(f) UK GDPR where the processing is necessary for the purposes of the legitimate interests of FBC but not where such interests are overridden by the interests or fundamental rights and freedoms of the **Data Subject** which require protection of **Personal Data**, in particular where the **Data Subject** is a child.
- 5.5 We may also process **Special Category** or criminal convictions etc data (“criminal offence data”) where it fulfils one of the substantial public interest conditions under Schedule 1, Part 2 of the Data Protection Act 2018, in particular, Conditions 10, 11, 12, 18 and 19.
- 5.6 We may also seek to obtain, use and retain criminal offence data in reliance upon Condition 31 relating to criminal convictions under Schedule 1, Part 3 of the Data Protection Act 2018.
- 5.7 For the purposes of Schedule 1, Part 4 of the Data Protection Act 2018, more information about FBC processing of **Special Category** and criminal convictions data under Conditions 10, 11, 12, 18, 19 and 31 can be found in the “Appropriate Policy Document” in Schedule 3 of this policy.
- 5.8 The processing of **Special Category** and criminal convictions data described in paragraphs 5.4 to 5.8 will only ever be carried out on the advice of statutory authorities, the Ministries Team of the Baptist Union of Great Britain or our Regional Association Safeguarding contact person.
- 5.9 Other data may also be considered ‘sensitive’ such as bank details but will not be subject to the same legal protection as the types of data listed above.

## **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 UK 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) the **processing** is necessary for us to perform a task in the **public interest** and the task has a clear basis in law;

- (e) the **processing** is **necessary for legitimate interests** pursued by FBC or another organisation, unless these are overridden by the interests, 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 UK 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 for **safeguarding 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 or persons we are in regular contact with in connection with our purposes;
- (d) the **processing** is necessary for **pursuing legal claims**.
- (e) 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 UK 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 in writing about who we are, our identity/contact details and those of the Data Protection Team, the reasons for **processing** and the legal basis, explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement, who we will share the data with, if we plan to send the data outside of the United Kingdom, how long the data will be stored and the **Data Subject's** rights.

This information is commonly referred to as a '**Privacy Notice**' and 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 section 6.5 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 under the UK GDPR 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.

If we plan to pass the data to someone else outside of FBChurch we will give the **Data Subject** this information before we pass on the data.

## **7. When we need consent to process data**

- 7.1 Where none of the other legal conditions apply to the **processing**, and we are required to get consent from the **Data Subject**, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for 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 specific purposes**

- 8.1 We will only process **Personal Data** for the specific purposes explained in our **Privacy Notices** (as described above in section 6.5) or for other purposes specifically permitted by law. We will explain those other purposes to **Data Subjects** in the way described in section 6 unless there are lawful reasons for not doing so.

## **9. Data will be adequate, relevant and not excessive**

- 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 that it was collected for. We will comply with official guidance issued to our sector 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) 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.

### **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, including their right to:

- (a) request access to any of their **Personal Data** held by FBC (known as a Subject Access Request);
- (b) ask to have inaccurate **Personal Data** changed;
- (c) restrict processing in certain circumstances;

- (d) object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
  - (e) data portability, which 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;
  - (f) not be subject to automated decisions, in certain circumstances;
  - (g) withdraw consent when we are relying on consent to process their data.
- 14.2 If a colleague 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 Team **immediately**.
- 14.3 We will act on all valid requests as soon as possible and at the latest within **one calendar month** from the date of receipt of the request, 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 plain language.

## 15. Direct Marketing

- 15.1 We will comply with the rules set out in the UK GDPR, the Privacy and Electronic Communications Regulations (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 FBC 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 and 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 legal exemptions apply to informing **Data Subjects** about the sharing. Only people authorised and properly instructed by the 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 measure 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 United Kingdom (UK)**

- 18.1 **Personal Data** cannot be transferred or stored outside of the UK unless this is permitted by the UK GDPR. This includes storage on a 'cloud' based service where the servers are located outside the UK.
- 18.2 We will only transfer data outside the UK where it is permitted by one of the conditions for non-UK transfers in the UK GDPR.

## **Section E – Managing change and 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 we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology and transferring data outside the UK. 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.
- 19.3 DPIAs will be conducted in accordance with the ICO's guidance on Data Protection Impact Assessments.

## 20. Dealing with data protection breaches

- 20.1 Where staff or volunteers, or contractors working for us, think that this policy has not been followed, or data might have been breached or lost, this will be reported immediately to the Data Protection Team.
- 20.2 We will keep records of **Personal Data** breaches even if we do not report them to the ICO.
- 20.3 We will report all data breaches which are likely to result in a risk to any person to the ICO. Reports will be made to the ICO within 72 hours from when someone in the Church becomes aware of the breach.
- 20.4 In situations where a **Personal Data** breach causes a high risk to any person we will, as well as reporting the breach to the ICO, inform **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 UK General data Protection Regulations (UK GDPR). The UK GDPR definitions are further explained below:

**Data Controller** means any person, company, authority or other body who (or which) determines the means for processing **Personal Data** and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The **Data Controller** is responsible for the **Personal Data** which is processed and the way in which it is processed. The Church Trustees are the **Data Controller** of data which we process.

**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. This definition will include the **Data Processors'** own staff (note that staff of **Data Processors** may also be **Data Subjects**).

**Data Subjects** include all 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) friends and family;
- (k) advisers and representatives or other organisations.

**ICO** means the Information Commissioner's Office which is the UK's regulatory body responsible for ensuring that we comply with our legal Data Protection issues. The ICO produces guidance on how to implement Data Protection law and can take regulatory action where a breach occurs.

**Personal Data** means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

**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 about that person, their actions and behaviour.

**Privacy Notice** means the information given to **Data Subjects** which explains how we process their data and for what purpose.

**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 UK 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.

**Schedule 2 – ICO Registration**

**Data Controller:** The Trustees of Folkestone Baptist Church

**Registration Number:** Z2053192

**Date Registered:** 13<sup>th</sup> January 2010 **Registration Expires:** 12<sup>th</sup> January 2024

**Address:** 135 Hill Road, Folkestone, Kent CT19 6LY.

## Schedule 3 – Appropriate Policy Document

### APPROPRIATE POLICY DOCUMENT – Folkestone Baptist Church.

#### Schedule 1, Part 4, Data Protection Act 2018: processing of special category and criminal offence data for the purposes of Parts 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018.

#### Who we are

Folkestone Baptist Church (FBC) is a fellowship of Christian believers in the Baptist tradition. For further information on what we do, please visit our website [folkestonebaptistchurch.org](http://folkestonebaptistchurch.org)

#### What this policy does

This policy explains how and why FBC collects, processes and shares **special category Personal Data** about you and data relating to criminal convictions etc in order to carry out our functions, in accordance with the data protection principles set out in the UK General Data Protection Regulation (UK GDPR.). Pursuant to Part 4 of Schedule 1 of the Data Protection Act 2018 (DPA 2018), **special category data** (Parts 1 and 2 of Schedule 1), and data relating to criminal convictions etc (Part 3 of Schedule 1), can only be processed lawfully if it is carried out in accordance with this policy. FBC staff, trustees and volunteers must therefore have regard to this policy when carrying out sensitive **processing** on our behalf.

#### Our approach to data protection

- FBC is committed to ensuring that the collection and processing of **Personal Data** is carried out in accordance with the UK GDPR and the DPA 2018.
- This is implemented through the provision of training for all staff, trustees and volunteers on data protection to ensure compliance with our policies and procedures.
- FBC values openness and transparency, and we have committed to and published a number of policies and processes to assist **Data Subjects** and to explain how we handle **Personal Data**. These include The FBC's Data Protection Policy, our Data Retention Schedule and **Privacy Notices** on our website [folkestonebaptistchurch.org](http://folkestonebaptistchurch.org) which describe what information we hold, why we hold it, the legal basis for holding it, who we share it with, and the period we will hold it for.
- FBC has appointed a Data Protection Team who have the day to day responsibility for ensuring that the information FBC collects is necessary for the purposes required and is not kept in a manner that can identify the individual any longer than necessary. Data protection training is provided for all new staff and volunteers and an annual update on data protection is provided to staff, trustees and volunteers, to ensure that everyone is familiar with FBC's data protection policies and procedures and in particular the **processing** of any **special category** and criminal offence data. The Data Protection Team will review any Data Protection Impact Assessments for FBC.



- Due to the nature of the activities performed by The FBC, we may need to share information with other organisations, for example the Baptist Union of Great Britain and The South Eastern Baptist Association and third parties, including statutory bodies and professional advisers, details of which can be found in our **Privacy Notice** at [folkestonebaptistchurch.org](http://folkestonebaptistchurch.org).

## **The data protection principles**

In summary, Article 5 of the UK GDPR states that **Personal Data** shall be:

- processed lawfully, fairly and transparently;
- collected for specific and legitimate purposes and processed in accordance with those purposes;
- adequate, relevant and limited to what is necessary for the stated purposes;
- accurate and, where necessary, kept up-to-date;
- retained for no longer than necessary, and
- kept secure.

## **Special category data and criminal convictions etc data**

### **Special category data:**

**Personal Data** refers to any information by which a living individual can be identified. Individual identification can be by information alone or in conjunction with other information. Certain categories of **Personal Data** have additional legal protections when being processed. These categories are referred to in the legislation as “**special category data**” and are data concerning:

- health
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- sex life or sexual orientation

## **Criminal convictions etc data:**

The **processing** of criminal convictions etc data also has additional legal safeguards. Criminal convictions etc data (“criminal offence data”) includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

## **Special category and criminal offence data we process about you**

FBC collects, processes and shares **special category** and criminal convictions data where it is necessary in order to carry out our functions. This **processing** is usually carried by the Designated Person for Safeguarding, the minister or certain charity trustees for the purpose of safeguarding against any risks posed to others in FBC or attending FBC activities by those who are involved in FBC, to mitigate the risk of individuals committing criminal offences (including of a sexual nature) and to assess individuals’ suitability for ministry or other work at FBC, including by reference to risks they may pose to others. These functions and the requisite processing of **Personal Data** are matters of substantial public interest.

If we process personal information about you, you are a “**Data Subject.**” Below is a non-exhaustive list of categories of **Data Subjects** who we might process information about:

- Employees, volunteers, workers or charity trustees of FBC;
- A child or individual in membership with or associated with FBC.

FBC will share this data with third parties only where strictly necessary (please see the section “Who we share your **Personal Data** with” below).

**Special Category** data and criminal offence data may be collected from the following non exhaustive list of sources:

- **Data Subjects;**
- Church members or individuals in regular contact with FBC including the minister, church officers, workers or volunteers, and the FBC’s Designated Person for Safeguarding;
- The Baptist Union of Great Britain (BUGB) Specialist Teams, in particular the BUGB Ministries Team and National Safeguarding Team;
- The South Eastern Baptist Association (SEBA) and, in particular, our SEBA Safeguarding contact person;
- Police, Social Services or the Local Authority Designated Officer for safeguarding.

FBC may also obtain and process this data for other statutory and legal obligations for example, including, but not limited to:

- > responding to data subject access requests under data protection legislation;
- > in connection with our duties under the Equality Act 2010.

## The legal basis for processing your special category or criminal offence data

**Privacy Notices** are available on the church website at [folkestonebaptistchurch.org](https://folkestonebaptistchurch.org). The **Privacy Notices** set out the legal bases for our processing of your **Personal Data**.

Where we process **Special Category** and criminal offence data it will be by reference to Article 6(1)(f) UK GDPR and Conditions 10, 11, 12, 18, 19 and 31 of Schedule 1 Data Protection Act 2018, which are described below:

Article 6(1)(f) UK GDPR, where the processing is necessary for the purposes of the legitimate interests of FBC, except where such interests are overridden by the interests or fundamental rights and freedoms of the **Data Subject** which require protection of **Personal Data**, in particular where the **Data Subject** is a child.

**Special Category** or criminal offence data may also be processed by FBC where it fulfils one of the substantial public interest conditions under Schedule 1, Part 2 of the Data Protection Act 2018:

(i) Condition 10:

Where the **processing** is necessary for the purposes of the prevention or detection of an unlawful act, it must be carried out without the consent of the **Data Subject** so as not to prejudice those purposes, and is necessary for reasons of substantial public interest.

In order to mitigate the risk of individuals committing criminal offences, including of a sexual nature, The FBC may undertake a risk assessment, receive, make a record of and share information about an individual who has been reported to us by another individual or a statutory authority, where there is a significant concern about their conduct and the risk they may pose to others.

(ii) Condition 11:

Where the **processing** is necessary for the exercise of a protective function, it must be carried out without the consent of the **Data Subject** so as not to prejudice the exercise of that function, and is necessary for reasons of substantial public interest. In this paragraph, “protective function” means a function which is intended to protect members of the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a body or association, or failures in services provided by a body or association.

FBC may exercise protective functions in partnership with BUGB’s Safeguarding and Ministries Teams or the Regional Association (SEBA), which include assessing individuals’ suitability for ministry or other work within the church including by reference to risks they may pose to others. These functions are discharged by custom, practice and with the consensus of the members of FBC, and the requisite **processing** of **Personal Data** is a matter of substantial public interest.

(iii) Condition 12:

Where the **processing** is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct, and in the

circumstances the **Data Controller** cannot reasonably be expected to obtain the consent of the Data Subject to the processing, and the processing is necessary for reasons of substantial public interest.

FBC may, in partnership with the Regional Association or BUGB, investigate and risk assess an individual's suitability for ministry or other work within or connected with FBC or the Baptist family, which is in the substantial public interest and forms an integral part of "generally accepted principles of good practice" as per the definition of "regulatory requirement" in Condition 12.

(iv) Condition 18:

Where the **processing** is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, the individual is aged under 18, or aged 18 and over and at risk, the **processing** is carried out without the consent of the **Data Subject** for one of the reasons listed in sub-paragraph (2), and (d) the **processing** is necessary for reasons of substantial public interest. (2) The reasons mentioned in sub-paragraph (1)(c) are – (a) in the circumstances, consent to the **processing** cannot be given by the **Data Subject**; (b) in the circumstances, the **Data Controller** cannot reasonably be expected to obtain the consent of the **Data Subject** to the **processing**; (c) the **processing** must be carried out without the consent of the **Data Subject** because obtaining the consent of the **Data Subject** would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

FBC may process criminal and **special category data** for the purposes of safeguarding minors and vulnerable persons or adults at risk.

(v) Condition 19:

Where the **processing** is necessary for the purposes of protecting the economic wellbeing of an individual at economic risk who is aged 18 and over and the **processing** is of data concerning health, is carried out without the consent of the **Data Subject** for one of the reasons listed in sub-paragraph (2), and is necessary for reasons of substantial public interest. An "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability. FBC may seek to rely on this condition if it is required to investigate allegations of financial abuse by an individual in ministry or other work or who is involved in the life of FBC, for the purpose of safeguarding vulnerable persons or adults at risk.

FBC may also seek to obtain, use and retain criminal offence data in reliance upon the following additional condition relating to criminal convictions under Schedule 1, Part 3 of the Data Protection Act 2018:

(vi) Condition 31:

where the **processing** is carried out by a not-for-profit body with a religious aim in the course of its legitimate activities with appropriate safeguards where it relates solely to the members or former members of the body or to persons in regular contact with it in connection with its purposes, and the **Personal Data** is not disclosed outside that body without the consent of the **Data Subjects**.

### **Who we share your personal data with**

We are required to share your data with third parties where we have a legal obligation to do so. We may also share information with our partner organisations with whom we have a Data Sharing Agreement, or as set out in our **Privacy Notices** available here: [folkestonebaptistchurch.org](http://folkestonebaptistchurch.org). The persons/organisations we may share your **special category** and criminal offence data with are:

- Our charity trustees, employees, contractors and volunteers on a need-to-know basis;
- The BUGB Specialist Teams;
- SEBA;
- Employees and volunteers working for one of our partner organisations with whom we have a Data-Sharing Agreement;
- Churches and other appointing or employing bodies as appropriate;
- Counsellors, professional supervisors and risk assessment consultants;
- The Police and Social Services, Local Authority Designated Officers and other statutory agencies;
- The Disclosure and Barring Service and our DBS Checking Company.
- Before sharing information with any of the above persons or organisations, careful consideration is given to the rights and freedoms of the **Data Subject** against what is needed to be shared to achieve our overarching goal of safeguarding children, young people and adults at risk from harm within FBC and to support and promote exemplary ministry. **Special Category** and criminal offence data is only disclosed where it is reasonably necessary to do so and a record and full details of any disclosure to third parties is maintained as follows:
  - (a) Membership List: in the custody of the Church Registrar.
  - (b) Church Address List (which distinguishes Members from regular worshippers):
  - (c) Criminal Records Data: in a locked safeguarding cabinet at FBC.

## **Automated decision making**

Currently FBC undertakes no automated decision making in relation to your **Personal Data**.

## **How we keep your data secure and how long we keep it for**

FBC deploys a range of technical and organisational measures to protect the **Personal Data** it holds and processes. Controls include but are not limited to:

- Regular data protection training for all staff and part of the induction for new staff;
- Robust procedures for the reporting of any data or potential data breaches.

These measures are under constant review by FBC.

The Church has a Data Retention Schedule which lists the data we hold and how long we hold it for. To find out how long we keep your data for, please see our Data Retention Schedule.

## **Your rights in relation to the data we hold**

Data protection legislation provides you with a number of rights relating to your **Personal Data**, including your special category and criminal conviction etc data. These rights are subject to some specific exemptions. Your rights may include:

- the right to access your data;
- the right to have your data corrected if it is wrong or incomplete;
- the right to request restrictions to the **processing** of your data;
- the right to object to your data being processed;
- the right to have your data erased;
- the right to be informed about how your data is processed;
- rights relating to automated decision making and data portability;

You should keep us informed of any changes to your information so that we can be confident that the data we hold about you is accurate. To understand more about these rights and how to exercise them please see our **Privacy Notice** on [folkestonebaptistchurch.org](http://folkestonebaptistchurch.org) and the Information Commissioner's Office website: [ico.org.uk](http://ico.org.uk).

## **Data Protection Team Contact**

Revd Katy Ruddle is the leader of the Data Protection Team and can be contacted by:

Telephone: 01303 252916

Email: [katy.ruddle@yahoo.co.uk](mailto:katy.ruddle@yahoo.co.uk)

Writing to: Folkestone Baptist Church, Hill Road, Folkestone, Kent CT19 6LY.

## **Your right to complain to the Information Commissioner**

If you are unhappy with any aspect of the way in which we have processed your **Personal Data**, you have the right to make a complaint to the Information Commissioner's Office by:

Telephone: 0303 123 1113

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk).

Writing to: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Website: [ico.org.uk](http://ico.org.uk)

## **Feedback or complaints about Folkestone Baptist Church, staff or volunteers**

If you want to give us feedback or make a complaint about FBC, its staff or volunteers in relation to the handling of your **Personal Data**, please contact Revd Katy Ruddle as above.

## **Review of this policy**

This policy will be regularly reviewed and may be subject to revision. Please visit our website to check for any updates.