Knaphill Baptist Church

DATA PROTECTION POLICY

Knaphill 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 3

1. Policy statement 3
2. Why this policy is important 3
3. How this policy applies to you & what you need to know 3
4. Training and guidance 4

Section B – Our data protection responsibilities 4

5. What personal information do we process? 4
6. Making sure processing is fair and lawful 5
7. When we need consent to process data 6
8. Processing for specified purposes 6
9. Data will be adequate, relevant and not excessive 7
10. Accurate data 7
11. Keeping data and destroying it 7
12. Security of personal data 7
13. Keeping records of our data processing 8

Section C – Working with people we process data about (data subjects) 8

14. Data subjects' rights 8
15. Direct marketing 8

Section D – Working with other organisations & transferring data 9

16. Sharing information with other organisations 9
17. Data processors 9
18. Transferring personal data outside the European Union (EU) 9

Section E – Managing change & risks 9

19. Data protection impact assessments 9
20. Dealing with data protection breaches 10

Schedule 1 – Definitions and useful terms 11

Schedule 2 – ICO Registration 13

Section A – What this policy is for

1. **Policy statement**

1.1. Knaphill 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 relevant laws, and adopting good practice.

1.2. 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 our Toddler Group;
(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) respond effectively to enquirers and handle any complaints

1.3. 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 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 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 & 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 Trustee 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; where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

3.2. **As a data subject of Knaphill Baptist Church:** We will handle your personal information in line with this policy.

3.3. **As an appointed data processor/contractor:** Companies who are appointed by us as a data processor 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 company, or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

3.4. **Our Data Protection Trustee** is responsible for advising Knaphill 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 the DP trustee at

Treasurer@KnaphillBaptist.org.uk.

3.5. Before you collect or handle any personal data as part of your work (paid or otherwise) for Knaphill 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.

3.6. 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 the Data Protection Trustee

4. Training and guidance

4.1. 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.

4.2. We may also issue procedures, guidance or instructions from time to time.

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, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers and other churches.

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[1]"** of data in the GDPR. This personal data can only be processed under strict conditions.

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. This processing will only ever be carried out on advice from the Ministries Team of the Baptist Union of Great Britain or our Regional Association Safeguarding contact person.

5.5. 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 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 Knaphill Baptist Church 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 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;

[1] '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.

(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 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: our identity/contact details and those of the Data Protection Trustee, the reasons for processing, and the legal bases, 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 European Union; how long the data will be stored and the data subjects' rights.

This information is commonly 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 section 6.5 as well as: the categories of the data concerned; and the source of the data.

6.7. 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 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.

6.8. If we plan to pass the data to someone else outside of Knaphill Baptist Church, 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 specified 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 for 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.

12.3. 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.

12.4. 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 us (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; and
(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 Trustee 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 and plain language.

15. **Direct marketing**

15.1. We will comply with the rules set out in the 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.

15.2. 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.

15.3. Any direct marketing material that we send will identify Knaphill 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 legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed 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 United Kingdom (UK)**

18.1. Personal data cannot be transferred (or stored) outside of the United Kingdom 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 & 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 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 Trustee.

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.

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 GDPR. The GDPR definitions are further explained below:

- **Personal data** means information relating to a living individual who can be identified from that data (or from that data plus other information in your possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal) or a statement of intention about them. From 2018 this also included 'online identifiers' such as computer IP addresses.

  The definition of personal data in data protection law includes two types of personal information about living individuals. This can be information held in electronic format or certain kinds of paper records or manual filing system.

- **Data subject** refers to the living individual whose personal data you hold. In a typical church situation this would include trustees, ministers, church members, members of the congregation, children in the Sunday School or Youth Group, and those attending Alpha courses etc. whose names and personal details are recorded.

  However, the definition also extends to all those living individuals whose personal information is held – even if this is only a name and email address or name and phone number. Therefore, complainants and casual enquirers who have no previous relationship with the church would be included within the definition if the church holds their name and any other details about them, as would those whose contact details are held because they relate to an individual who provides a service to the church (such as an electrician, for example).

- **Special Category Data** is personal data which the UK GDPR says is more sensitive and so needs more protection. This was previously known as 'Sensitive Personal Data' and is information concerning the data subject's race or ethnic origin, politics, religion, trade union membership, health, sex life or sexual orientation. In addition, genetic data and biometric data (e.g. fingerprint data or data obtained through facial-recognition technology) now also fall into this category although it is highly unlikely that churches will hold any such data!

  Much of the information which churches are likely to process will be sensitive personal data as it is likely to concern the data subject's religious beliefs. Information relating to the physical or mental health of church members, employees, volunteers and other individuals may also be held by a church.

- **Criminal Offence Data** is personal data relating to criminal convictions and offences. Under the UK GDPR this is a separate category of data. Churches may, for example, be told about convictions which relate to the safeguarding of children and adults at risk, including the preparation of a Safeguarding Contract with a church member.

- **Data Processing** refers to the operations carried out on personal data. The usual processing operations are: Collecting - Editing - Storing/holding - Disclosing - Sharing - Archiving - Viewing (e.g. personal data on an electronic device or in paper records) - Recording - Listening to (e.g. a voicemail message left Page 5 of 24 by a church member) - Erasing/deleting. During the 'life cycle' of personal data, several different processing operations can be carried out in relation to that data – from its initial collection to its eventual erasure and removal from church electronic or paper records. If the church – or people working for the church in a paid or unpaid capacity - holds personal information electronically or in organised paper records, you will be processing it. In a typical church situation, there could be several individuals who process personal data on behalf of the church. This may include:
    - Minister – processing members' personal data for pastoral reasons
    - Church treasurer – holding bank details of individuals to whom expenses are paid
    - Church administrator – maintaining the church's contact list or Directory
    - Youth Club leader – holding emergency contact details of parents
    - Safeguarding administrator – holding references and other information about those who are working with children and adults at risk in the church.
- **Data controller** refers to the person or persons (i.e. legal person) who determines the purpose and the manner by which personal data is to be processed. This is the name of the legal entity which holds the personal data. In the case of an unincorporated Baptist church, the data controller will be the charity trustees* (usually the minister, deacons and elders or Leadership Team). In the case of churches which are registered with the Charity Commission as either Charitable Incorporated Organisations (CIOs), or as Companies Limited by Guarantee (CLG) - then the data controller will be the CIO or the CLG.

  It is important to note that the definition of data controller also includes all staff and volunteers who work for the church. Therefore, when staff and volunteers process personal data in their role within the church they will be processing as the data controller entity.
- **Data processor** refers to the legal person who processes the personal data on behalf of the data controller and under their instructions. This 'person' will be a third party e.g. an individual (such as a sole trader or self-employed person) or another organisation which is asked by the church to carry out some kind of processing on their behalf. The key point is that for the third party to be deemed a data processor (rather than a separate data controller) they must be processing the personal data for the church's purposes and not their own business purposes. The staff who work for the data processor entity also fall within the definition.
- **Privacy notice** means the information given to data subjects which explains how we process their data and for what purposes.
- **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.

Schedule 2 – ICO Registration

Knaphill Baptist Church is considered to be exempt from registration:

Churches are currently exempted from notification if the processing

a) is carried out by the church, that is under the direction of the Charity Trustees or others appointed by the Church Members' Meeting (the Data Controller)

b) is for the purposes of establishing or maintaining membership of the church or for support of the church, or for administering activities for individuals who are either members of the church or have regular contact with it; (this is the exempt purpose)

c) is of personal data in respect of which the data subject is:-

   i) a past, existing or prospective member of the church or its associated organisations;

   ii) any person who has regular contact with the church or its associated organisations in connection with the purposes: or

   iii) any person the processing of whose personal data is necessary for the exempt purposes

d) is of personal data consisting of the name, address and other identifiers of the data subject or information as to:

   i) eligibility for membership of the church or its associated organisations;

   ii) other matters the processing of which is necessary for the exempt purposes;

e) does not involve disclosure of the personal data to any third party other than:

   i) with the consent of the data subject; or

   ii) where it is necessary to make such disclosure for the exempt purposes: and

f) does not involve keeping the personal data after the relationship between the data controller and the data subject ends, unless and for so long as it is necessary to do so for the exempt purposes.

Date	By	Notes	Date Agreed
23rd September 2018	Church Meeting	Adopted	23rd September 2018
24th March 2020	AGM	Reaffirmed	24th March 2020.
7th March 2022	Eric Moore	Reformatted and tidied Section 18 reworded to reflect UK leaving European Union	
28th March 2023	AGM	Reaffirmed	
29th March 2024	Eric Moore	Review: Definitions updated in line with BU Guidance	
27th Feb 2025	AGM	Reaffirmed	27th Feb 2025
9th March 2025	Eric Moore	Minor review and cosmetic corrections	
11th April 2026	Eric Moore	Minor updates in line with BU Guidance	14th April 2026