SLOUGH BAPTIST CHURCH POLICY	Data Protection Policy
POLICY NUMBER: SBCP-35	

Primary Responsibility:	Church Secretary

Issued:	May 2019
Status:	Final
Review Period:	3 years
Next Review Date:	May 2022

DISTRIBUTION

Original	Slough Baptist Church Office
Copy	Website (PDF)

1. Purpose and Scope of this policy document

The purpose of this document is to define how the church will implement the roles and processes required by the General Data Protection Regulation (GDPR) and other data protection laws.

The scope of this document is the outline of key roles and principles. This document does not contain a copy of the legislation (which is described on the government website in many pages), nor does it include all the details of the processes (which will be in separate church documents).

2. Types of Personal Data

The GDPR applies to '***personal data***'.

Personal data means information relating to a living individual who could be identified from that data (or from that data in combination with other data being used by the church). 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.

It is important to note that personal data is not limited to the church's computer database and paper filing systems. Some personal data is unstructured, for example in photos, videos, texts, or voicemail. This unstructured data is stored in a variety of ways, some examples being on a piece of paper, a mobile phone, a USB stick, an email or a text message.

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.

There are more details in Appendix A about personal data, special categories and ***other sensitive data***.

3. Overall Intent

Slough Baptist Church will protect the personal data entrusted to it and will ensure that each type of data is used only for its proper purposes. The church will uphold the rights of the people whose personal data we collect and use (***Data Subjects' Rights***). The church will comply with all data protection legislation and will adopt good practice.

4. Registration with the Information Commissioner's Office

The church will renew registration with the ***ICO*** annually. Registration details are as follows:

- Registration Number: Z7160034
- Date First Registered: 04 November 2002
- Data Controller: SLOUGH BAPTIST CHURCH

5. The role of the Trustees

The Trustees will be the ***Data Controller*** for Slough Baptist Church, meaning that they will have a responsibility to define:

- the purposes for the church's processing of personal data
- how it is processed.

The Trustees will be responsible for putting into place comprehensive but proportionate governance measures. They will be accountable by law for demonstrating that the church complies with the principles of data protection described in the legislation. The way the Trustees will fulfil their responsibilities and demonstrate compliance is by implementing the policy outlined in this document.

6. The role of the Data Protection Coordinator

The Trustees will appoint a Data Protection Coordinator to inform and advise the church and its employees and suppliers about their obligations to comply with the GDPR and other data protection laws. Therefore, the Data Protection Coordinator will be required to be familiar with the laws and keep up to date with any changes. Other aspects of the Data Protection Coordinator's role are described in the relevant sections of this policy.

The Data Protection Coordinator will report to the Trustees. The Trustees will ensure that the Data Protection Coordinator is able to operate independently and is not dismissed or penalised for performing their task, and that adequate resources are provided to enable them to meet their GDPR obligations.

The current Data Protection Coordinator is Matt Warren.

7. The role of Data users

The staff and volunteers at the church who handle ***personal data*** are required to perform their ***processing*** of this data in line with the GDPR. In practice this means complying with this policy and the associated procedures.

8. The role of Data Processors

Any third parties who do processing on behalf of the church (***Data Processors***) will be required to perform their ***processing*** of this data in line with the GDPR

Before appointing a contractor, 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.

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.

Where we have existing contracts or informal working arrangements, we will amend them to ensure compliance with the GDPR.

9. The Data Protection Register

We will keep a Data Protection Register in order to ensure that all usage of data within the church is being appropriately protected. The register identifies how and where data is being used, including:

- Description (e.g. Gift aid forms)
- Purpose (in line with section 13 below)
- Legal basis for processing the data
- Who uses the data
- Where it is kept
- How long it is kept
- Any actions required

The Data Protection Register is the key document for many other data protection processes, such as identifying data users who need to be trained, data that needs deleting, secure storage requirements and so on. Because it is so important to the overall protection of data, the Data Protection Register will be reviewed at least twice a year by the Data Protection Coordinator and the Church Manager in order to ensure it is up to date and that the actions required are being carried out. The date of each review will be recorded in the register.

10. Auditing data protection compliance

The Data Protection Coordinator is responsible for monitoring compliance with data protection law.

To assist with this, and to show how we comply with the law, we will keep clear records of our processing, for example records of consent, records of when data has been reviewed for deletion, and when people have been trained.

We will also make available for inspection this policy, our GDPR procedures and documentation about data protection actions taken and planned to be taken.

11. The Procedures for Data Protection

We will ensure Data Protection by implementing documented ongoing operational procedures, which will include procedures for:

- Training data users
- Collecting data and obtaining consent to use it
- Storing data securely
- Deleting data
- Providing people with details about the data the church holds about them
- Responding to requests for data subject access
- Reporting data breaches to the Information Commissioner's Office
- Auditing data protection compliance

12. Training and guidance

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. We will also issue guidance to volunteers who handle personal data on behalf of the church.

13. The purposes for the church's processing of personal data

The church will ***process*** personal data only for the following purposes:

1. Membership, attendance and the newsletter (e.g. birthdays & anniversaries)
2. Pastoral care for those connected with the church
3. Services to the community (e.g. Parent & Toddler groups)
4. Safeguarding children, young people and adults at risk
5. Staff management (e.g. appraisals)
6. Volunteer management (e.g. rotas)
7. Financial governance (e.g. Gift Aid)
8. Publicity – including our website
9. Maintaining the security of our property and premises
10. Responding effectively to enquirers and handling any complaints
11. Legal requirements (e.g. the marriage register)

Any other purpose (e.g. if someone wished to write a book about people in the church) is not covered by existing policy or procedures, and therefore must first be authorised by the Trustees in their role as Data Controller.

14. Making sure processing is fair and lawful

Processing of ***personal data*** will only be fair and lawful when the purpose for the processing meets a legal basis (see Appendix B), and when the processing is transparent.

The lawful basis for each use of data will be recorded in the Data Protection Register. This will normally align with the conditions shown in Appendix B, but when necessary we will refer to the text of the GDPR, or to any relevant guidance, or seek legal advice.

To be transparent, we will provide people with an explanation of how and why we process their personal data at the point we collect data from them. This will take the form of a reference to our ***privacy notice*** via our website or office. When we collect data from other sources, we will similarly inform the people affected at the point we collect the data.

15. Informing people before we use data about them

If ***personal data*** is collected directly from the individual, we will inform the person (the '***data subject***') about:

- The legal entity who will hold the data
- How to contact the Data Protection Coordinator
- The reasons for processing, and the legal bases
- Details of our legitimate interests, explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement
- Whether the data will be shared, and if so with whom
- Whether the data will be stored outside of the European Union
- How long the data will be stored
- Their rights (***data subjects' rights*****)**

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

The privacy notice will be stored on our website, and a printed copy will be stored in the office. The form used to collect the data will describe how to view the privacy notice.

If data is not collected directly from the individual, we will provide the data subject with the information in the list above and also:

- The categories of the data concerned;
- The source of the data.

This information will be provided to the individual in writing no later than one 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.

If we plan to pass the data onto someone else outside of Slough Baptist Church, we will give the data subject this information before we pass on the data.

16. Obtaining consent to process data

Unless we are legally permitted to process the personal data, we will request consent from the ***data subject***. We will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent will be specific to each process.

When requesting consent, we will explain

- What we are asking consent for
- Why we are collecting the data
- How we plan to use it.
- Their rights as data subjects to withdraw consent at any time
- How to withdraw consent

We will ensure that it is as easy to withdraw consent as to give it.

17. Data will be relevant and not excessive

We will only collect and use personal data that is needed for the specific purposes described in this policy. 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.

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 (such as safeguarding any people in our church who may be put at risk, or protection of members of the public). This type of data processing will only ever be carried out after seeking advice from the Baptist Union.

18. Accurate data

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.

19. Destroying data

We will destroy data as soon as practicable when legitimately requested to do so by a ***data subject***.

We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with official guidance about retention periods for specific records.

We will record in the Data Protection Register how long we will keep the data.

20. Security of personal data

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

In choosing appropriate measures, we will take into consideration:

- the quality of the security required
- the costs of implementation

- the nature, scope, context and purpose of processing
- the risk (in terms of likelihood and severity) to the rights and freedoms of data subjects
- the harm that could result from a data breach

Technical security measures will include where appropriate:

- Passwords and encryption
- Secure systems backup
- Physical security of the premises

Organisational security measures will include where appropriate:

- Minimising access to data
- Training and guidance
- Audits, reviews and testing

21. Direct Marketing

"***Direct Marketing***" is described in Appendix A.

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 and telephone (whether live calls or recorded messages).

Any direct marketing material that we send will identify Slough 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.

22. Responding to requests for data subject access

Access is one of the ***Data Subjects' Rights*** described in Appendix A.

Anyone may request the details of the data held about them by the church, and what it is used for. The Data Protection Coordinator will be informed of the request, which will be responded to within one calendar month, unless there is a need and a lawful basis to extend the timescale. There will be no charge for providing the information, and the information will be concise and transparent, using clear and plain language.

23. Dealing with data protection breaches

We will instruct all staff, volunteers, and contractors using personal data to report immediately to the Data Protection Coordinator any instances where they think that this policy has not been followed, or that data protection might have been breached or data lost.

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

We will report all data breaches that 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.

24. Changes to Data Processing

The Data Protection Coordinator will be responsible for approving any changes to the way the church processes data, ensuring that data is protected by design and default. In the case of major changes, this will include preparing a Data Protection Impact Assessment (DPIA) for the Trustees to approve. DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'. Any decision not to conduct a DPIA will be recorded.

25. Sharing data with other organisations

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 staff and Trustees are allowed to share personal data.

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.

26. Transferring personal data outside the European Union

We will only transfer personal data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU.

Appendix A. Definitions of GDPR terms

Data Controller	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. We are the data controller of data which we process
Data Processors	Any individuals or organisations that 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 Subject	Any living person whose personal data we process. 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) the employees of our contractors; d) volunteers; e) tenants; f) trustees; g) complainants; h) supporters; i) enquirers; j) friends and family; k) advisers and representatives of other organisations.
Data Subjects' Rights	The GDPR names the following rights for Data Subjects: a) **The right to be informed** – to be given a clear explanation of why and how we process their personal information b) **The right of access** – to see what data we hold and how we are processing the data, so they can verify the lawfulness of the processing c) **The right to rectification** – to have inaccurate personal data corrected d) **The right to erasure** (or "right to be forgotten") – to have data about them deleted e) **The right to restrict processing** – their data remains, but is not processed f) **The right to data portability** – to receive their data in an easily usable computer format g) **The right to object** – including preventing the use of their data for direct marketing or research h) **Rights in relation to automated decision making and profiling** – to request a human to be involved if the decision will have a significant or legal effect on them The GDPR also mandates the **right to withdraw consent**.

Direct Marketing	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, nor be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation’s aims.
ICO	The **Information Commissioner’s 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.
Other sensitive data	Other data, such as bank details, may also be considered ‘sensitive’ but will not be subject to the same legal protection as the ‘**special categories’** of data described below.
Personal Data	Any information relating to a natural person (living person) who is either identified or is identifiable. Personal data can be factual (for example, a name, address, date of birth, education or employment history) or it can be an opinion about that person, their actions and behaviour. This includes data we receive directly from the person, 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. Personal data may be in electronic or paper form. It also applies to photos or videos of people. 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 personal data	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.
Privacy Notice	The information given to data subjects which explains how we process their data and for what purposes
Processing	**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 moving or still images that can identify living individuals is also a processing activity.

Appendix B. Lawful uses of personal data and special categories of data

Personal data

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:

1. the processing is necessary for a contract with the data subject;
2. the processing is necessary for us to comply with a legal obligation;
3. the processing is necessary to protect someone's life (this is called "vital interests");
4. the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
5. the processing is necessary for legitimate interests pursued by the church or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.
6. If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

Special categories of data

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:

1. the processing is necessary for carrying out our obligations under employment and social security and social protection law;
2. 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;
3. 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;
4. the processing is necessary for pursuing legal claims.
5. If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.