Bromley Baptist Church

INTERNAL DATA PROTECTION POLICY

Updated version formally adopted: 2 June 2020

Bromley Baptist Church is committed to protecting all information that we handle about people we support and work with, and to respecting their rights around how their information is processed. This Policy sets out our responsibilities and how we will meet them and is written for internal use. It is complemented by an external facing Data Protection Policy and Privacy Notice which summarises these provisions. The protection of Personal Information needs to be set in the context of a fast-moving Information Revolution and therefore this Policy and its accompanying privacy notices and procedures will be reviewed at regular intervals to ensure all are kept up to date. This document is based on advice from the Baptist Union.

Contents

Section A – What this policy is for

1. Policy statement

1.1 Bromley 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.

We process personal data to help us:

a) maintain lists of our members and other individuals who interact with us

b) provide a contact list and other services for our members

c) safeguard children, young people and adults at risk

d) recruit, support and manage staff and volunteers

e) maintain our accounts and records, including those relating to gifts

f) promote our activities

g) maintain the security of property and premises

h) respond effectively to enquirers and handle any complaints.

1.2 This policy has been approved by the Trustees who are responsible for ensuring that we comply with all our legal obligations. It explains how we will go about fulfilling our responsibilities whenever we obtain, store or use personal information, however it is stored.

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 an individual needs to do to ensure the church complies with the relevant legislation and good practice.

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 **Employees, trustees, members, group leaders and volunteers.** You are required to comply with this policy and must be particularly careful if you are processing personal information on behalf of the church, for example keeping details of group members, or if you are given a church contact list.

3.2 All church and church group procedures and policies must complement the requirements of this Policy. If anyone is in doubt about whether anything they plan to do, or are currently doing, might breach this policy then they should speak to the Data Protection Officer.

3.3 If you think that you have accidentally breached this policy it is important that you contact the church's Data Protection Officer immediately so that swift action can be taken to try and limit the impact of the breach.

3.4 It is important to note that you can be personally liable for any breaches and in serious cases this could lead to prosecution, action from the regulator (the Information Commissioner) or internal disciplinary action. The Data Protection Officer (see section 15) is available, training will be given regularly and see appendix three for a summary of your responsibilities.

3.5 **People connected with our church**. We might hold your personal information because you attend one of our activities or have asked to be kept informed of our work. Individuals for whom we hold personal information are assured that we are making every effort to manage their personal information in line with this policy.

3.6 **Companies who are appointed by us.** All companies that have any access to our data will be required to comply with this Policy under their 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.

3.7 **The Data Protection Officer.** The DPO (see 'governance in section 15) is responsible for advising the church and its staff, trustees and volunteers 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.

Section B – Our data protection responsibilities

4. What personal information do we process?

4.1 In the course of our work, we will collect and process information (personal data) about many different people (data subjects). This includes information we receive directly 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 or organisations working with the families and individuals we support.

4.2 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.

4.3 We hold types of information that are called **"special categories"** of data in the GDPR. This personal data can only be processed under strict conditions.

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

4.4 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.

4.5 Other data may also be considered 'sensitive' such as bank details.

5. Making sure processing is fair and lawful

5.1 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?

5.2 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 Bromley 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?

5.3 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

c) the processing is carried out in the **course of our legitimate activities** and only relates to 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**.

5.4 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?

5.5 If personal data is collected directly from an individual or their parent/guardian, we will inform them about:

a) our contact details

b) the reasons for processing and the legal basis (including explaining any automated decision making or profiling)

c) our legitimate interests

d) the consequences of not providing data needed for a contract or statutory requirement

e) who we will share the data with

f) if we plan to send the data outside of the European Union

g) how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice' (see Appendix 1) and our privacy notice is publicly available on our website.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described above 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 **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 our church, we will give the data subject this information before we pass on the data.

6. When we need consent to process data

6.1 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.

6.2 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.

7. Processing for specified purposes

7.1 We will only process personal data for the specific purposes explained in our privacy notices (as described above in section 5.5) 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.

8. Data will be adequate, relevant and not excessive

8.1 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.

9. Accurate data

9.1 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.

10. Keeping data and destroying it (our data retention schedule)

10.1 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.

10.2 Each person or group holding personal information should review what is held on an annual basis during the months of July and August to ensure they are only keeping data which is required. Data that is not required will be deleted or destroyed. The Data Protection Officer will offer advice as appropriate.

10.3 We will ensure that personal information that must be kept for legal requirements ((eg financial and employment details) will be kept (even if people have left the church.)

10.4 Three years is considered to be appropriate for keeping personal information after the closure of an active 'pastoral care' intervention in the cases of people remaining within the church or leaving (but this will be synchronised with safeguarding retention requirements.)

11. Security of personal data

11.1 We 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.

11.2 Our security measures must provide a level of security appropriate to the risks involved in the processing. Measures 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.

11.3 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.

12. Keeping records of our data processing

12.1 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)

13. Data subjects' rights

13.1 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

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

13.2 If anyone 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 Officer immediately as well as informing the appropriate manager or group leader.

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

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

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

14. Direct marketing

14.1 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.

> **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.

14.2 Any direct marketing material that we send will identify Bromley 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 – how we deliver data protection in Bromley Baptist Church

15. Governance

15.1 The Operations and Development Manager, Janet Law, is the nominated Data Protection Officer. The church also has a trustee responsible for data protection (Jude Mackenzie). The DPO will:

a) Organise, with the safeguarding lead, regular training for group leaders and trustees.

b) Ensure that new group leaders are given information on their data protection responsibilities.

c) Remind group leaders to 'clean' their data files annually (usually in July/August.) This means deleting any out of date information.

d) Schedule an annual review by the trustees of this policy.

e) Ensure that members are reminded annually of their responsibilities, for example, at a church meeting.

16. Training and guidance

16.1 We will provide general training at least annually for all staff, trustees and volunteer leaders to raise awareness of their obligations and our responsibilities, as well as to outline the law. Guidance and appropriate instruction will also be provided for trustees and volunteers. This may be done as part of training for other areas such as safeguarding.

16.2 We may also issue procedures, guidance or instructions from time to time. Managers/leaders must set aside time for their teams to look together at the implications for their work.

Section E – working with other organisations and transferring data

17. Sharing information with other organisations

17.1 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 staff can share personal data.

17.2 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.

18. Data processors

18.1 Sometimes we may appoint external companies that will use our data on our behalf (for example to print and mail out some invitations or to manage some financial processes.) For the purposes of the legislation these are called 'data processors'. Before doing this, 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.

18.2 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.

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

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

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

19.3 We will take account of any procedural changes required by the UK's exit from the European Union.

Section E – Managing change and risks

20. Data protection impact assessments

20.1 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 EU. Any decision not to conduct a DPIA will be recorded.

20.2 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.

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

21. Dealing with data protection breaches

21.1 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 Officer.

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

21.3 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.

21.4 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.

Appendix 1 – **Bromley Baptist Church General Data Protection Policy and Privacy Notice**

Bromley Baptist Church is committed to protecting all information that we process about our members and other individuals we support and work with, and to respecting people's rights around how their information is handled.

This policy explains our responsibilities about personal information and how we will meet them. It also serves as a general Privacy Notice that explains how we hold and process personal information. It is complemented by a detailed internal policy which details how the policy is implemented within our church. This is available on request.

The protection of personal information needs to be set in the context of the fast-moving information revolution and therefore our policies and procedures will be reviewed at regular intervals to ensure they are kept up to date.

This policy is also consistent with our other organisational policies and practices including those concerned with Confidentiality and Safeguarding. This policy governs our general use of personal information such as for newsletters and ad hoc communication with members, regulars and other people who have close contact with the church.

We hold and share information in accordance with legal rights. The Data Protection Act 1998 was brought into force to protect an individual's privacy. From May 2018, this has been replaced by the General Data Protection Regulation (GDPR). This means each individual should know, or be able to find out, why we need to use personal information and with whom we share the information. Individuals are also entitled to know how long their personal information will be held for and that the information is accurate.

Everyone has the right to ask us to remove information that is not covered by one or more of the other grounds listed in the Data Protection Regulation (eg. we hold a record of donations via gift aid). Individuals can write, phone or email us to request this. Once this request is confirmed, the church will immediately stop processing and/or sharing that information and will remove the data as appropriate from the records as soon as reasonably possible.

The reasons we process personal information are to:

a) maintain lists of members and other individuals who interact with the church. For example, individuals who make donations or request information and the provision of a contact list to members
b) provide pastoral support to families and individuals
c) safeguard children, young people and adults at risk
d) recruit, support and manage staff and volunteers
e) maintain our accounts and records, including those relating to gifts
f) promote our activities
g) maintain the security of property and premises
h) respond effectively to enquirers and handle any complaints.

In particular, we will make sure that all personal information is:

a) processed lawfully, fairly and with due regard to the need for confidentiality
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 individuals regarding their personal data.

Sometimes information needs to be shared with other organisations and this will be in accordance with good practice and the relevant data protection regulations. When appropriate, consent will be obtained from individuals and they will be informed about how and when information is shared. We will only share information with organisations when we have confidence in their data protection procedures.

We process personal information in both electronic and paper form. The personal data we process can include information such as names and contact details, education or employment details, and visual images of people. We hold types of information that are called 'special categories' of data. For example, religious faith is a special category as is other information that is processed as a result of pastoral support. This personal data can only be processed under strict conditions.

'Special categories' of data (as referred to in the General Data Protection Regulation) include 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.*

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. 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.

The church maintains a contact database including names, addresses, email and telephone details of members and friends. This information may be made available to those listed within it by request – in either printed or electronic format. Individuals aged 13 years and over will be required to give their consent to be included which will include their agreement and understanding that their information will be shared with others listed. The church will provide advice about the safekeeping of this information and individuals will need to agree to follow this as part of their agreement for inclusion.

Should you have any questions about our policy and procedures please contact our church administrator, Dave Brown: office@bromleybaptist.com 020 8460 3307.

Last updated: June 2020

Appendix 2

Bromley Baptist Church

Protection of personal information

Summary advice for members, volunteers and group leaders

People trust Bromley Baptist Church to keep their private information safe and confidential. This includes their contact details and personal information about themselves such as health information.

The 'privacy notice' on our website and our internal policy describe in detail how we, as a church, adhere to the laws that keep this information safe.

This page is a quick summary of what you need to know if you are a trustee or group leader in our church.

Try where possible to use the church database of information and cascade system rather than your own. The church database and email distribution meets all the legal requirements of gaining consent, clarity about source, and how to opt out. You can keep details on your own devices for people but, if you are representing the church, you must still obey the law. As a rule of thumb, if your list contains people you don't know, or don't know you, you shouldn't be keeping it separately.

In most cases you cannot pass on or share someone's personal information unless they have given their consent.
Examples: You hold contact details of people who are part of a women's group so that you can let them know about meetings and events. Your friend who runs an organic vegetables company asks for the contact list so she can send them details of a special offer. You cannot share their details without their written consent.

You must keep people's personal information safe and secure.
Examples: You have kept details on your computer of people who are part of your church prayer group . Your computer is shared with other members of the family. You should password protect the prayer group details.

If someone wants you to delete their personal information you must do so (and tell the church office)
Example: A member of your housegroup moves to a new church. They tell you they don't want any information from our church from now on. You take them off the group email list for housegroup and you let the church office know so that they don't receive our regular emails any more.

There are special rules if someone is at risk.
If you are worried that someone is at risk, for example a child or a vulnerable adult, you are then legally allowed to share personal information. However, in these instances, unless it is an emergency, you must speak to the safeguarding lead Glenis Ruston in the first instance.

Don't store information that you don't need
Your role as group leader makes it relevant for you to keep names and email addresses. It doesn't allow you to store details of other factors. The law is particular protective of information like ethnicity, sexuality and health profile. Full details of this are in the main church policy.

If you have any concerns or questions contact our Data Protection Officer (Janet Law). This includes questions from someone about what information we hold, and if you lose your laptop or phone, or suspect someone has got hold of the personal information you have. If this happens we need to let people know.

Appendix 3

Summary of duties of the Data Protection Officer and lead trustee

The Data Protection Officer and lead trustee are responsible for ensuring that the church keeps to this policy and stores, uses and protects personal data legally and efficiently (section 15). This page is a key to some of the main responsibilities.

5.5	When we collect data from people we must make sure we let them know key information about how it will be used and protected. This can be by linking to the privacy policy on our website. And, generally, we must let people know before any of their information is released to another person or organisation.
8.1	Make sure we only collect information that we need. We can't collect other information 'just in case'.
9.1	Make sure we have processes in place to check the accuracy of our information.
10.2	Once a year (July and August) cull the church data for out-of-date records, and prompt group leaders to do this, too. Group leaders that cease to be leaders should also delete personal information that they hold.
10.3	Make sure that information is retained for the correct length of time if needed for legal reasons such as employment or financial reasons.
10.4	Pastoral information should be kept for three years.
12.1 and 17.2	Oversee a process to record our data processing decisions and actions, including for any times we share data with another organisation.
14.2	Ensure that we comply with the rules for our email cascades.
16.1&2	Arrange annual training and any ad hoc training required during the year.
20.1	Ensure impact assessments are done before we take any actions that have implications for data protection.
21	Oversee a process for dealing with breaches of the policy, including rapid reporting to the ICO where necessary.
	Ensure that trustees review this policy annually.

Appendix 4 – Definitions and useful terms (taken in entirety from the Baptist Union template Policy)

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

Data controller means any person, company, authority or other body who (or which) determines the means 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 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 of other organisations.

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.

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 purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

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

l) Racial or ethnic origin;

m) Political opinions;

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

o) Trade union membership;

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

q) Genetic data;

r) Biometric data;

s) Sexual life and sexual orientation.

Appendix 5 – ICO Registration details

Data Controller: Bromley Baptist Church

Registration Number: Z6465998

Date Registered: 11 March 2002 **Registration Expires:** 10 March 2021

Address: Bromley Baptist Church, Park Road, Bromley BR1 3HJ