Ballee Baptist Church

Data Protection Policy

CONTENTS

1. POLICY STATEMENT

1.1 Ballee Baptist Church ("we") is a charity which has the purpose of advancing the Christian faith according to Biblical principles. We are registered as a data controller with the Information Commissioner's Office (ICO), registration number Z2846614, and process the personal information of individuals in accordance with our principal charitable Purpose and our constitution.

We process personal data to enable us to:

(i) Provide a voluntary service for the benefit of the public as specified in our constitution;
(ii) Administer membership records;
(iii) Manage our employees and volunteers;
(iv) Maintain our own accounts and records;

1.2 Everyone has rights with regard to the way in which their personal data is handled. In line with our values and aims, we are committed to good practice in the handling of personal and confidential information and to ensuring that such information is stored securely and is processed in accordance with the law.

2. PURPOSE OF THIS POLICY

2.1 In the course of our work, we will collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners and others).

2.2 We process the personal information of individuals in both electronic and paper form and all this data is protected under data protection law. In some cases, it is sensitive information about individuals' religious or other beliefs, finances and personal circumstances. In addition, we hold lots of less sensitive information such as names and contact details, employment details, visual images of members; current, past and prospective staff; volunteers; advisers; complainants and enquirers; representatives of other organisations; as well as business and other contacts such as suppliers. We do not hold information relating to criminal proceedings or offences. We may also receive other personal information from the above or other sources.

2.3 We are aware that individuals can be harmed if their personal information is misused, is inaccurate, if it gets into the wrong hands as a result of poor security or if it is disclosed carelessly. We are committed to protecting personal data and information from unauthorised disclosure and ensuring its accuracy.

2.4 The purpose of this policy is to set out what measures we are committed to taking, as an organisation and as individual members of staff (including volunteers), to ensure we comply with the relevant legislation including:

(i) The General Data Protection Regulation (GDPR);
(ii) The Privacy and Electronic Communications Regulations (EC Directive) (PECR);
(iii) Any other laws and regulations relating to the protection of personal data.

2.5 Breaches of data security or confidentiality are serious incidents. If they occur, they will be investigated fully and actively managed to ensure that any breach is as limited as possible. A breach of the GDPR, or other legislation may mean that we, and/or a member of our staff or volunteer, are liable to prosecution or to regulatory action. We may also be required to report breaches to the Information Commissioner's Office (ICO) if a breach results in a risk to an individual, and to inform the data subject if the breach results in a high risk to any person.

3. DEVELOPMENT OF THIS POLICY

3.1 This policy has been approved by the Charity Trustees. It sets out the legal rules which apply whenever we obtain, store or use personal data.

3.2 The Church Secretary is responsible for the development of policies and procedures relating to data protection, ensuring compliance with data protection legislation and the investigation and resolution of any breaches of data security. Any questions about the operation of this policy or any concerns that this policy has not been followed should be referred to the Secretary at secretary@balleebaptist.org. The Secretary will:

(i) Keep the content and effectiveness of this policy under review;
(ii) Oversee compliance with the policy;
(iii) Keep a record of all data security incidents or breaches and investigate in appropriate detail;
(iv) Provide or arrange training and guidance for staff;
(v) Act as our nominated contact with the ICO.

3.3 From time to time we may need to make changes to this policy or guidance in line with current operational practices and/or legislation.

3.4 Any questions, ideas or concerns about the operation of this policy or recommendations for additions or amendments should be referred to the Secretary.

4. TRAINING AND GUIDANCE

We will provide general training for all staff and volunteers involved in handling data to raise awareness and outline the law. We may also issue guidance or instructions from time to time.

5. HOW THIS POLICY APPLIES TO YOU

5.1 **As an employee/volunteer:** You are required to comply with this policy under your employment or worker contract. If you find that you have accidentally breached the policy it is important that you contact the Secretary immediately so that the impact of the breaches can be assessed. Anyone who breaches the data protection policy may be subject to disciplinary action, particularly in the following circumstances:

(i) There is a big gap between the person's practice and what this policy requires;
(ii) Data subjects have been placed in significant risk of suffering damage and/or distress;
(iii) There is a data security breach; or
(iv) The person has breached the policy intentionally, recklessly, for personal benefit or in concert with others.

5.2 **As an appointed data processor/contractor:** if you are appointed by us as a data processor you are required to comply with this policy. Any breach of the policy will be taken seriously and could lead to enforcement action. 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.

5.3 **As a data subject (see definition at 6.2 below):** We will use your personal information in accordance with this policy.

5.4 If you are unsure about whether anything you propose to do might breach this policy you must speak first with the Secretary.

6. DEFINITIONS OF DATA PROTECTION TERMS

The GDPR (and this policy) "applies to

(i) the processing of personal data wholly or partly by automated means and

(ii) to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

The first part covers all data processing which involves the use of a computer ('processing' broadly covers all forms of handling of data, including storing and accessing it. The term is defined in more detail below).

The second part covers processing which does not involve a computer, of data which either forms part of a filing system, regardless of how well-structured it is, or which is collected in order to be added to a filing system at a later time (e.g. notes of a telephone conversation which are intended to be transferred to a file), even if the data is not actually added.

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

6.2 **Data subjects** include all living individuals about whom we hold or otherwise process personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects for whom we are likely to hold personal data include:

(i) Our employees;
(ii) Members, Adherents and volunteers;
(iii) Children (attending youth ministries) and their parents/guardians
(iv) Singers and guest speakers;
(v) Consultants/Individuals who are our contractors or employees working for them;
(vi) Complainants;
(vii) Enquirers;
(viii) Advisers and representatives of other organisations.

6.3 **Personal data** means any information relating to a natural 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. In addition, personal data is limited to information about living individuals and does not cover deceased persons.

An 'identified' natural person is one who is identified from the data. An 'identifiable natural person' on the other hand is one who is not identified from the data itself but who can be identified, directly or indirectly, by reference to other data, such as an identification number, location data, an online identifier or to one or more factors specific to that person.

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.

6.4 **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 such decisions are taken alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. The Charity Trustees of Ballee Baptist Church are the data controller of data which we process and this policy is intended to explain how we will comply with the GDPR.

6.5 **Data processors** include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provided secure waste disposal for us. This definition will include the data processors' own staff (note that, as mentioned above, staff of data processors may also be data subjects).

6.6 **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.

6.7 **Sensitive personal data** (referred to as 'special categories of data' in the GDPR) includes information about a person's:

(i) Racial or ethnic origin;
(ii) Political opinions;
(iii) Religious or similar (e.g. philosophical) beliefs;
(iv) Trade union membership;
(v) Health (including physical and mental health);
(vi) Genetic data;
(vii) Biometric data;
(viii) Sexual life and sexual orientation.

Information relating to criminal convictions and offences cannot be processed unless the processing is authorised by law or is carried out under the control of official authority. This includes information about (i) allegations of criminal offences; (ii) proceedings in relation to criminal offences or alleged offences; and (iii) the disposal of criminal proceedings including sentencing. Sensitive personal data can only be processed under strict conditions, including the data subject's explicit consent (although other alternative conditions can apply in limited, very specific circumstances).

7. DATA PROTECTION PRINCIPLES

7.1 Anyone processing personal data must comply with the GDPR's Principles. These provide that personal data must be:

(i) processed lawfully, fairly and in a transparent manner (see Section 8.6 below);
(ii) processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;
(iii) adequate, relevant and limited to what is necessary for the purpose;
(iv) accurate and, where necessary, up to date;
(v) not kept longer than necessary for the purpose, unless it is retained for public interest, scientific, historical research or statistical purposes and appropriate measures are taken to safeguard the rights of data subjects;
(vi) processed in a manner which ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational means.

7.2 Personal data must also be processed in accordance with the rights of data subjects (see Section 14 and Schedule 1).

7.3 Personal data cannot be transferred (or stored) outside the European Economic Area (EEA) unless this is permitted by the GDPR (see Section 19). This includes storage on a cloud the servers of which are located outside the EEA.

8. FAIR AND LAWFUL PROCESSING

8.1 Fairness of processing means that we only process data in the manner in which data subjects reasonably expect. In order to make data subjects aware of how we process personal data, the GDPR requires that we provide data subjects with certain information when we collect information from them as well as when we collect information about them from other sources.

8.2 If personal data is collected directly from data subjects, we will inform them (in writing) about:

(i) Our identity and contact details;
(ii) The identity and contact details of the person to whom data protection queries and concerns should be addressed;
(iii) The purposes for which we intend to process the data and the legal basis for the processing;
(iv) If data processing is justified on the basis of legitimate interests pursued, those legitimate interests should be identified;
(v) The recipients, or categories of recipients of the data;

(vi) The period for which the data will be stored or the criteria for determining that period;
(vii) The rights of data subject as set out in Schedule 1;
(viii) Where processing is based on consent, the right to withdraw that consent at any time;
(ix) The right to complain to the Information Commissioner's Office;
(x) Whether the provision of personal data is a contractual or statutory requirement, the possible consequences of failing to provide it;
(xi) If we intend to process personal data further for a purpose other than that for which the data was collected we will also provide information on that purpose prior to the further processing.

This information must be given at the time when the personal data is obtained.

8.3 If data is collected otherwise than directly from the data subjects we will provide to the data subjects (in writing), within a reasonable time and not later than one month after we collect the data, with the information described in paragraph 8.2 as well as the following information:

(i) The categories of data concerned;
(ii) The source of the personal data.

If we use personal data collected in this manner for communicating with data subjects we must provide this information not later than the time of our first communication with them, and if we intend on disclosing any of the personal data we must provide this information before the disclosure.

If we collect data from the data subject and we are aware that we will later be collecting additional data from third party sources it may be more effective to provide all the information to the data subject when we collect the data from them.

8.4 The information described in paragraphs 8.2 and 8.3 must be given in clear and plain language, and must be concise, transparent, intelligible and easily accessible. Depending on the context, it may be appropriate to provide the more essential information and explain where the full information can be found.

8.5 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter, unless a legal exemption under the DPA applies. Legal advice should be sought before an exemption is applied and a record must be kept of a decision to apply an exemption including the reasons for it.

8.6 Processing of data is only lawful if at least one of the conditions listed in article 6 of the GDPR is satisfied. These conditions include:

(i) The data subject has given consent to the processing of the data for specific purposes (as described in Section 9);
(ii) The processing is necessary for a contract with the data subject;
(iii) The processing is necessary for us to comply with a legal obligation;
(iv) The processing is necessary for legitimate interests pursued unless these are overridden by the interests, rights and freedoms of the data subject.

The GDPR includes other conditions and before deciding on which condition should be relied upon, the original text of the GDPR should be consulted as well as any relevant guidance.

8.7 When we rely on the legitimate interests ground we must carry out a balancing exercise, weighing our legitimate interests with the rights of the individuals concerned. If our use of that information poses a risk to the rights of the individual it may be more appropriate to obtain the individual's consent for the particular processing so as to give the individual more control over how we use their information.

8.8 When sensitive personal data is processed, we must also satisfy one of the conditions set out in article 9 of the GDPR. These include:

(i) The data subject has explicitly given consent;

(ii) The processing is necessary for carrying out our obligations under employment and social security and social protection law;
(iii) 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;
(iv) The processing is necessary for pursuing legal claims.

The GDPR provides other alternatives for processing sensitive personal data as well and before deciding on which condition should be relied upon, the original text of the GDPR should be consulted together with any relevant guidance.

8.9 It is important that decisions we make concerning which grounds we will rely on are recorded.

9. CONSENT

9.1 Where personal data is not necessary for contractual purposes or for our legitimate interests or in the absence of a legal obligation justifying processing, usually the consent of the data subject is required to justify processing. Consent can however be withdrawn at any time and if withdrawn, the processing should cease. Data subjects should be informed of their right to withdraw consent and withdrawing consent should be as easy as it is to provide consent.

9.2 The GDPR requires consent to be a freely given, specific, informed and unambiguous indication of the data subject's wishes. It must be a statement or clear affirmative action which signifies agreement to the processing of personal data relating to the member. As a result, presumed consent and pre-selected opt-in boxes will not constitute valid consent under the GDPR.

9.3 Consent cannot be relied on if the individual concerned does not have a choice whether to provide us with their information or not. We cannot therefore require consent as a condition to providing a service as consent would not be considered to be freely given (other grounds for processing may be useful in such a case).

9.4 When obtaining consent we are also required to clearly set out the specific reason why we are obtaining the individual's information and how we intend to use it so that the individual's consent can be considered specific and informed.

9.5 Consent is not everlasting and before obtaining consent for processing personal data we should consider how we can ask the individual to refresh their consent at reasonable intervals in the future. Although the law does not specify how long consent is valid for, in determining this we will take into account how long the individuals concerned can expect their data to be used for. As an example, if we obtain consent from an individual to use their image that individual might reasonably not expect us to use their image more than a year later.

9.6 It is not enough that we obtain consent but we must be able to show that we obtained consent. It is therefore best to obtain consent in writing so that we can keep a clear and durable record of it.

10. PROCESSING FOR SPECIFIED PURPOSES

10.1 We will only process personal data for the specific purposes set out in our privacy notices (as described in Section 8) or for other purposes specifically permitted by law. We will notify those purposes to the data subject in the manner described in Section 8 unless there are lawful reasons for not doing so and this is permitted by a legal exemption.

10.2 We may process data for further purposes which we might not have envisaged when providing the data subject with the original privacy notice as long as the further purpose is compatible with the original purpose for which the data was collected. When assessing compatibility we will consider, among all other relevant issues, the link between the purposes, the context in which the data was collected, the reasonable expectation of the data subject concerned, the nature of the personal data, the consequences of the further

processing and the existence of appropriate safeguards. We are required to inform data subjects of the further purposes and provide them with appropriate additional information before we commence the further processing.

11. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

11.1 We will only collect and use personal data to the extent that it is required for the specific purpose described in Section 8 above (which would normally be notified to the data subject). We should collect and use just enough information, which is relevant, to achieve that purpose, but not more than is required.

11.2 We will check records regularly for missing information and to reduce the risk of irrelevant or excessive information being collected.

11.3 When implementing systems which involve processing personal data we will consider how such systems can provide for data minimisation by design and by default as described in Section 22.

12. ACCURATE DATA

12.1 We will ensure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data should be checked at the point of collection and at regular intervals afterwards. If a data subject informs us of a change of circumstances their record must be updated as soon as is practicable. All reasonable steps will be taken to destroy or amend inaccurate or out-of-date data.

12.2 Data subjects are to be given the means to easily contact us to amend any data which we hold about them if it is inaccurate or outdated and we should effect such changes unless we have a good reason not to.

12.3 Where a data subject challenges the accuracy of their personal data, we will mark this information as potentially inaccurate and we will try to resolve the issue informally. Where the issue is not resolved, disputes will be referred to the Secretary.

12.4 Records should be kept in such a way that the individual concerned can inspect them. Such documents could also be required, in certain circumstances, to be disclosed to other bodies at a later date. Information should therefore be correct, unbiased (unless a professional opinion is required to be given), unambiguous and clearly readable. Information from an external source should be recorded clearly and dated, and the source identified.

13. DATA RETENTION AND DESTRUCTION

13.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and we will comply with official guidance issued to our sector with regard to retention periods for specific items of personal data. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

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

13.3 When they are no longer required, solid state devices, hard disks, CD-ROMs and other storage media which have at any time held or processed personal data must be dealt with so that the personal information cannot be recovered from them. They should be overwritten using a process approved by our IT team so that the data previously stored on them is beyond recovery by any available technological or other means, or should be physically destroyed by secure means.

14. PROCESSING IN ACCORDANCE WITH DATA SUBJECTS' RIGHTS

14.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(i) Request access to any personal data held about them by us (the right of subject access is discussed in Section 15 below),

(ii) Ask to have inaccurate personal data amended; and
(iii) Object to processing, in certain circumstances.

14.2 If any communication is received by a member of staff from a data subject which relates or could relate to their data protection rights, this should be forwarded to the Secretary **immediately**.

14.3 A more detailed description of the rights of data subjects can be found in Schedule 1 although the precise conditions contained in the GDPR will be applied when giving effect to these rights.

15. DIRECT MARKETING

15.1 'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This includes contact made by organisations to individuals solely for the purposes of promoting their aims and the advertising need not be of a commercial product, nor need anything be offered for sale. We will adhere to the rules set out in the GDPR, the Privacy and Electronic Communications Regulations and any laws which may amend or replace the rules governing direct marketing when we make contact with data subjects, whether that contact is made by (but not limited to) post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Stricter rules apply to marketing by email and other electronic means including text messaging, social media messaging, fax and automated telephone calls.

15.2 Any direct marketing material that we send should identify us as the sender and should describe how an individual can object to receiving similar communications in the future.

15.3 Data subjects have a very strong right to object to any form of processing of their personal data for a direct marketing purpose. If an individual exercises their right to object we are required to cease processing for this purpose within a reasonable time.

16. DEALING WITH SUBJECT ACCESS REQUESTS

16.1 All data subjects have a right to obtain from us copies of personal data which we hold about them. Such copies shall be provided together with information about:

(i) The purposes of processing;
(ii) The categories of personal data concerned;
(iii) The recipients to whom the data has been or will be disclosed, particularly if these are outside the European Economic Area;
(iv) The envisaged period for which the data will be held;
(v) The existence of the right to request rectification, erasure or restriction of processing as well as the right to object to data processing;
(vi) The right to lodge a complaint to the ICO;
(vii) Where the data is collected from someone other than the data subject, the source from which we obtained the data;
(viii) The existence of any automated decision-making and a description of the logic involved as well as information about the significance and envisaged consequences of such processing;
(ix) The safeguards in place in relation to personal data transferred outside the European Economic Area.

16.2 Requests do not need to be made in any particular form and need not quote the law or the right of subject access. It is enough that a data subject asks for their personal information. Staff who receive such a request must forward it to the Secretary immediately as there is a limited timeframe in which we are required to comply and we may need to obtain additional information from the individual before we can do so, including clarification of the scope of the request and confirmation of the individual's identity.

16.3 More information about the right of subject access can be found in Schedule 1.

16.4 We do not and cannot charge a fee for complying with a subject access request save in exceptional circumstances described in Schedule 1.

16.5 Except in limited circumstances when complying with a subject access request we may not disclose the personal data of third parties. For this reason personal data of third parties should be redacted from documents which are provided to the requester.

16.6 The right of subject access (SAR) is a right of the individual and is therefore only exercisable by that particular individual. The information should also only be provided to that individual. The exception to this rule is when a request is made by a person other than the data subject on behalf of the data subject and:

(i) The data subject has authorised the requester to make the request on their behalf and to receive the information; or
(ii) The data subject is incapable of understanding the nature and implications of a subject access request.

With regard to requests made by children or on behalf of children, as a rule of thumb, a child of 12 or over is usually regarded as capable of possessing the requisite mental capacity, although this is not an absolute indicator and decisions in this regard will depend on the mental and emotional development of the child in question.

16.7 Where we have reasonable doubts as to the identity of the requester we will seek to verify their identity before any personal data is disclosed. Evidence of legal authority to act on behalf of the data subject will be required where a request is made on behalf of someone else.

16.8 Evidence of identity of the data subject and any third party acting on their behalf can be established by production of a combination of the following (in original or certified copy):

(i) Passport;
(ii) Photo driving licence;
(iii) Utility bill showing current address;
(iv) Birth/marriage certificate;
(v) P45/P60.

16.9 Evidence of legal authority to act on behalf of an adult can include:

(i) Original signed letter of authority from the data subject (where the data subject possesses full mental capacity);
(ii) Original or certified copy of a relevant power of attorney or Court of Protection Deputyship Order (where the data subject lacks mental capacity).

16.10 In certain circumstances, exemptions may apply which may require or allow us to withhold information requested in response to a subject access request although it should be presumed that all personal data relating to an individual should be disclosed to them. Legal advice should be sought when it is thought that an exemption may be applicable.

16.11 We will keep records of all subject access requests and a record of why information was redacted or withheld (e.g. subject to an exemption).

16.12 Further information on dealing with subject access requests can be found on the website of the Information Commissioner's Office (ICO).

17. DISCLOSURES OF INFORMATION TO THIRD PARTIES (DATA SHARING)

17.1 All personal data is held securely by us and will be treated in a confidential manner. We will only disclose personal data when we have legal grounds to do so and if we have previously informed the data subject about the possibility of similar disclosures (in a privacy notice), unless legal exemptions apply. Only authorised and properly instructed members of staff are permitted to make external disclosures of personal data. These disclosures may include:

(i) Disclosures made in accordance with a legal obligation, such as a court order or statutory duty;

(ii) Disclosures made in order to enforce or apply any contract with the data subject; or

(iii) Disclosures made to protect our rights, property, or safety of our employees, volunteers, contractors or others. This includes exchanging information for the purposes of the prevention or detection of crime.

17.2 We will keep records of all information supplied in response to a request for disclosure by a third party and will carefully document any exemptions which may have been applied (including the reasons for their application). Legal advice may need to be obtained in appropriate cases.

17.3 We will abide by the ICO's statutory ***Data Sharing Code of Practice*** (or any replacement code of practice) when sharing personal data with other data controllers.

18. SECURITY OF PERSONAL DATA

18.1 We will process personal data in a manner that ensures that it is kept appropriately protected and secure, including from unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical and organisational measures which include as a minimum those described in this Section 18.

18.2 We will implement appropriate technical and security measures which ensure a level of security of processing which is appropriate to the risk of processing.

In assessing the appropriateness of technical and organisational measures we shall take into account:

(i) the nature, scope, context and purpose of processing;

(ii) the risk (of varying likelihood and severity) for the rights and freedoms of natural persons;
the costs of implementation.

In assessing the appropriateness of the level of security we shall, among other relevant considerations, take into account the risks that are presented by the processing involved, in particular the risks which could result from a personal data breach.

18.3 We will put in place policies, measures, procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. These may include:

(i) Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(ii) Measures to ensure that we are able to restore availability and access to personal data in a timely manner if there is a physical or technical incident;

(iii) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

18.4 The security measure we put in place include:

(i) Physical Security

Appropriate building security measures such as alarms and lockable cupboards, smoke detectors and fire alarms.

(ii) Systems Security

• Security software is installed on all computers containing personal and/or confidential data;
• Only authorised users are allowed to access computer files and passwords are required to be both strong and regularly changed. Staff and others to whom systems access is granted should never share their password with any other person;
• Only a limited portion of the personal information that we control will be available for all staff to use: most staff will have limited access to personal and confidential data – on a 'need to know', role-appropriate basis;

• The servers and infrastructure which form our IT network will be kept in locked rooms and cabinets. Only qualified IT employees and IT contractor staff may access the physical servers and infrastructure;
• All non-portable user devices will be encrypted and so far as possible, portable devices such as laptops, memory sticks and portable hard drives will be encrypted;
• Computer files are regularly backed up and copies kept securely;
• Persons who process personal data on our behalf ('data processors') will be vetted before we appoint them and we will not appoint them unless we are satisfied that they are able to process data in a manner which meets the requirements of the GDPR and provides protection for the rights of data subjects. Data processors will only be engaged by means of written contracts which contain the provisions required by the GDPR;

(iii) Organisational Security

- Staff and volunteers will undergo regular data protection training and must adhere to the terms of this policy;
- Staff and contractors shall be subject to a legally binding duty of confidentiality;
- All paper documents containing personal data should be locked away in cabinets and not left out overnight;
- Paper documents which are required to be destroyed shall be securely shredded. Digital storage devices should be physically destroyed when they are no longer required;
- The identity of callers shall be checked before any personal information is provided to the caller. If it is not possible to do so, the caller should be directed to contact us in writing or in person. Staff should refer to the Secretary in difficult situations and should not feel compelled to disclose information when it is not appropriate to do so.

19. TRANSFERRING PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

19.1 We may only transfer personal data we hold to a country outside the EEA if this is permitted under the GDPR. This includes situations where we upload personal data to a cloud the servers of which are situated outside the EEA.

19.2 Under the GDPR, we are permitted to transfer data outside the EEA in certain circumstances. These include situations where we transfer data:

(i) To a country or international organisation which the European Commission declares, by means of a decision, to be a country or international organisation which provides an adequate level of protection (provided that the relevant decision remains in force);
(ii) Pursuant to a contract which incorporates model contractual clauses which are issued by the European Commission or the ICO in accordance with the GDPR;
(iii) Pursuant to contractual clauses which are authorised by the ICO;
(iv) The data subject explicitly consents to the transfer, which consent shall be of the level required in Section 9 of this policy and the GDPR;
(v) The transfer is necessary for one of the reasons set out in Article 59 of the GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

19.3 Satisfying one of the conditions in paragraph 19.2 does not eliminate the need to comply with all other requirements for processing personal data.

19.4 When we use the services of a cloud service provider (or any other data processor) which requires data to be processed outside the EEA we must ensure that we satisfy one of the conditions contained in this Section 19 of this policy (or alternatives provided under the

GDPR) as well as comply with the requirements relating to the appointment of data processors described in Section 24 on this policy.

20. DEALING WITH DATA PROTECTION BREACHES

20.1 Where staff, or contractors working for us, consider that this policy has not been followed the matter should be reported immediately to the Secretary. These include, among others, situations where:

(i) an unauthorised person may have gained access to personal data;
(ii) personal data (including copies and backups of it) has been lost, even if temporarily;
(iii) data has been uploaded onto an unsecure server, including a server situated outside the EEA if this is not done in accordance with the relevant GDPR requirements;
(iv) a computer or other device on which personal data is accessible is affected by a virus or other malicious code;
(v) personal data becomes corrupted or is accidentally altered;
(vi) any login details where discoverable for a period of time;
(vii) a direct marketing email is sent in a manner which allows recipients to view the email addresses of others;
(viii) a power outage or other similar incident results in personal data not being accessible for a period of time.

20.2 We must keep records of personal data breaches, even if we do not report them to the ICO, and such records must be such as to enable the ICO to verity our compliance with the GDPR. The records will be kept by the Secretary and will describe, as a minimum:

(i) The facts relating to the personal data breach;
(ii) Its effects; and
(iii) Remedial action taken.

20.3 We are required to report all data breaches which are likely to result in a risk to any person, to the ICO. Reports must be made within 72 hours from when we become aware of the breach and the time limit starts to run from when any member of staff or contractor becomes aware of the breach and not when the Secretary becomes aware. For this reason, it is very important that incidents are reported to the Secretary immediately so that he or she can decide if a report should be made.

20.4 Reports to the ICO shall contain the following information:

(i) A description of the personal data breach including the categories of and number of data subjects and records concerned;
(ii) The name and contact details of the Secretary and other persons from whom the ICO can obtain more information;
(iii) The likely consequences of the data protection breach;
(iv) The measures taken or proposed to be taken to address the personal data breach including measures to mitigate the possible adverse effects.

20.5 In situations where a personal data breach causes a high risk to any person, we shall, in addition to reporting the breach to the ICO, inform the data subject whose information is affected, without undue delay. This can include situations where, for example, information containing bank account details is left unattended in a public place 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. When informing data subjects, we will, as a minimum, provide them with the information described in 20.4(ii), 20.4(iii) and 20.4(iv) above.

20.6 Since the timeframe within which we must report personal data breaches could start to run from the moment a contractor becomes aware of a personal data breach, we must make sure that in all our contracts with contractors, we require them to provide us with the information listed in paragraph 20.4 above immediately upon discovering a potential

breach, as well as to provide us with any additional information we may require to comply with our data protection obligations.

20.7 When a data protection breach occurs, the Secretary shall consider the following:

(i) Does this policy require amending?
(ii) Should further guidance be issued about this policy?
(iii) Do any members of staff require additional training or guidance?
(iv) Is it appropriate to take disciplinary action?

21. RECORD KEEPING

21.1 The GDPR requires that organisations not only comply with the law but are able to show that they comply with the law. It is therefore very important that we keep clear records of all processing activities and decisions we make concerning personal data (setting out our reasons for those decisions). Although the GDPR lists specific records which should be kept this does not reduce our responsibility to ensure that we are able to prove compliance with the law at all times.

21.2 The GDPR specifically requires that we keep, as a minimum, the following records about our processing activities:

(i) The name and contact details of any joint controller, any representative and/or data protection officer;
(ii) The purpose of the processing;
(iii) A description of the categories of data subjects;
(iv) A description of the categories of personal data;
(v) The categories of recipients to whom the personal data have been or will be disclosed;
(vi) Transfers to countries or organisations outside the EEA (including their identification) and any relevant safeguards;
(vii) The envisaged time limits for erasure of the different data;
(viii) A description of security measures taken.

21.3 The GDPR also requires data processors to keep records and should we appoint a data processor we shall require them, in the contract by which they are appointed, to keep such records and to give us access to such records when we require it.

22. DATA PROTECTION BY DESIGN AND BY DEFAULT

22.1 We will implement appropriate technical and organisational measures to ensure that all personal data is processed in accordance with the GDPR, primarily the principles of data protection described in this policy. This includes having safeguards built into our systems which provide for compliance by default. As an example, forms which we use for recording personal data should provide for inputting all relevant data but no extra information. This is referred to as data minimisation.

23. DATA PROTECTION IMPACT ASSESSMENTS

23.1 Before carrying out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment. These include situations when we process data relating to vulnerable people, trawling of data from public profiles and data transfers outside the EEA. We may also conduct a DPIA in other cases when we consider it appropriate to do so. Any decision not to conduct a DPIA should be recorded.

23.2 DPIAs should be carried out early enough to allow recommendations to be acted upon and a DPIA should be continuously be carried out on existing processing activities. A DPIA should be reassessed at least every three years, depending on the nature of the processing and the rate of change in the situation.

23.3 All DPIAs should involve the Secretary and his advice and decisions shall be documented.

23.4 When carrying out a DPIA we will consult with the data subjects concerned and if we decide not to do so we shall keep a record of such a decision (including reasons).

23.5 If we are unable to mitigate the identified risks such that a high risk remains we are required to consult with the ICO.

23.6 DPIAs shall be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments' and the European 'Guidelines on Data Protection Impact Assessment'.

24. APPOINTING DATA PROCESSORS

24.1 Should we decide to appoint a contractor to process personal data on our behalf (a data processor) we will, before appointing them, carry out a due diligence exercise to ensure that the relevant processor will implement appropriate technical and organisational measures to ensure that the data processing will meet the requirements of data protection law, including keeping the data secure, and will ensure protection of the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do so.

24.2 We will only appoint data processors on the basis of a written contract which must contain provisions which require the processor to:

(i) Process the personal data only on our documented instructions;
(ii) Ensure that persons authorised to process the personal data have committed themselves to confidentiality;
(iii) Take all measures required in relation to security of processing;
(iv) Not appoint sub-processors without our prior written authorisation and equivalent contractual obligations;
(v) Assist us to fulfil our obligations to give effect to the rights of data subjects;
(vi) Assist us in complying with our legal obligations, in particular those relating to security, breach notification and communication with data subjects, and carrying out data protection impact assessments;
(vii) At our choice, delete or return all personal data after the end of the provision of services relating to the processing, and delete existing copies unless longer storage is required by law;
(viii) Make available to us all information necessary to demonstrate compliance with our obligations in relation to appointing data processors;
(ix) Allow us to conduct, and assist us in conducting, audits, including inspections of the processors, which may be carried out by us or an auditor of our choosing;
(x) Inform us if an instruction we give to the processor breaches any data protection law.

24.3 In addition to the provisions listed in paragraph 24.2 above it may be appropriate for us to require a data processor to comply with our policies, maintain records, provide us with information and otherwise generally assist us to comply with our data protection obligations (see, for example, Section 21 above).

24.4 It should be noted that it is not enough to have the clauses listed in paragraph 24.2 above included in a contract with the processor and we will remain liable for breaches of data protection law committed by the data processor unless we can show that we were not in any way responsible for the event giving rise to the damage. We would not be able to show this unless we carry out the due diligence exercise mentioned in paragraph 24.1 above and unless we carefully monitor the data processing throughout the duration of the contract.

25. CHANGES TO THIS POLICY

25.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or by email.

Schedule 1 - Rights of data subjects

Under the GDPR data subjects have various rights. These are described below.

Please note that the descriptions below are only intended to be used as guidance and do not, in any way, affect how they apply under the GDPR. We will apply the rights in accordance with the GDPR which overrides the text of this schedule.

Those who wish to obtain more information about this procedure or their data protection rights generally may contact the Secretary: secretary@balleebaptist.org.

1. Right of Access

Data subjects have a right to access personal data about them which we hold. It is not a right to documents, but only to personal data contained in documents. This does not cover personal data which relates to other persons.

Under the GDPR, requests must be complied with without undue delay and, in any event, within one month of the request. This time limit can be extended to two months where necessary, taking into account the complexity and number of requests. For an extension to apply the data subject must be informed of the extension and why it is needed within one month of the request.

If the request is made electronically, the information should be provided in a commonly used electronic form.

If more than one copy of the data is requested, we may charge a reasonable fee based on our administrative costs for providing the extra copies. If a request is manifestly unfounded or excessive, we are entitled to refuse to comply with the request or to charge a reasonable fee (based on administrative costs) to deal with the request. We must inform the data subject about this and explain to the data subject that they have a right to complain to the ICO. We will not apply this exception unless we have a strong justification to do so.

2. Right to Rectification

Data subjects may request that we rectify any inaccurate information concerning them and we will comply with such requests as soon as practicable. Data subjects also have a right to have incomplete personal data concerning them completed.

3. Right to Erasure (to be forgotten)

Data subjects are entitled to have their personal data deleted if:

(i) it is no longer needed;
(ii) the only legal ground for processing is consent and the data subject withdraws consent;
(iii) the data subject objects to processing (see the Right to Object below) and there are no overriding legitimate grounds to continue with the processing;
(iv) the data has been processed unlawfully;
(v) the data has to be erased for compliance with a legal obligation which applies to us.

There are exceptions to this right. These include when processing is required for compliance with the law, reasons of public interest, research or statistics, and legal claims.

4. Right to Restrict Processing

Data subjects can in some circumstances demand that processing of their personal data is restricted for a limited time period. The personal data would continue to be held on record, but it cannot otherwise be processed without the data subject's consent. The limited circumstances and time periods are:

(i) if the accuracy of the data is contested, for a period which enables us to verify the accuracy of the data;
(vi) if the processing is unlawful and the data subject opposes the erasure of the data but requests restriction of its use instead;
(vii) if we no longer require the data but the data subject needs the data for the establishment, exercise or defence of legal claims;
(viii) the data subject has objected to data processing (see the Right to Object below), until an assessment is made of whether there are overriding legitimate grounds which can justify the continuation of the processing.

Even if the data subject exercises this right we are entitled to process the data in question for purposes relating to legal claims, for the protection of the rights of other persons or for reasons of public interest.

We must inform the data subject when the restriction will be lifted.

5. Right to Object

Where data is processed for the performance of a task carried out in the public interest or legitimate interests pursued by us or a third party, data subjects may object to the processing on grounds relating to their particular situation. In such a case, we will stop processing that data unless there are compelling legitimate grounds for the processing to continue or if the processing is required in connection with legal claims.

Data subjects can object to the processing of their data for purposes of direct marketing. This is an absolute right and the processing should cease on request.

When data is processed for research or statistical purposes, data subjects can object on grounds relating to their particular circumstances, unless the processing is required for reasons of public interest.

6. Right of Data Portability

Data subjects have a right to receive personal data which they provide to us in a structured, commonly-used, and machine-readable (digital) format and are entitled to transmit that data to any other person if the processing of that data is carried out by automated means and is based on 1. the data subject's consent or 2. is processed out of necessity for the purpose of performing a contract with the data subject. Data subjects may also request that we transfer their data directly to a third party.

This right only applies to personal data which data subjects provided to us in a structured digital format.

7. Other Rights

Other rights of data subjects in relation to their personal data which arise under the GDPR consist of the right:

(ix) To be provided with privacy notices;
(x) To request information about persons to whom their personal data has been disclosed;
(xi) To withdraw consent to processing which is based on consent.
Withdrawing consent should be as easy as it is to give consent.
Withdrawal of consent does not affect the lawfulness of processing already carried out;
(xii) To make a complaint to the Information Commissioner's Office (https://ico.org.uk/);
(xiii) Not to be subject to decisions based solely on automated data processing which significantly affect them or which produce legal effects concerning them.

8. Exercising rights

Data subjects who wish to exercise any of the above rights or who have any questions about them should contact our Secretary: secretary@balleebaptist.org.

Any information provided to data subjects should be provided in a concise, transparent, intelligible and clearly accessible form, using clear and plain language.

We are required to provide information on action taken subsequent to a request by a data subject based on the above rights, without undue delay and within one month from when we receive the request. This can be extended by two further months where necessary, depending on the complexity and number of requests. If an extension is required, we must inform the data subject within one month of receiving the request and give reasons for the delay.

We may refuse to comply with requests that are manifestly unfounded or excessive or, alternatively, we may charge a reasonable charge based on our administrative costs. If no action is to be taken, the data subject must be informed of that fact and the reasons within one month from the date of the request. The data subject must also be informed of their right to make a complaint to the ICO.

If a request is made by electronic means, all information shall be provided by electronic means where possible, unless otherwise requested by the data subject.