MINEHEAD BAPTIST CHURCH

DATA PROTECTION POLICY

Adopted at the Church Members' Meeting 15th May 2018, Schedule 2 amended 12th June 2018

Minehead Baptist Church (hereinafter called "The Church") is committed to protecting all information that it handles about its members, people it supports and works with and to respecting people's rights as to how their information is handled. This policy explains those responsibilities and how they will be met.
In this document the words "Church" and "we" are used interchangeably and all members fall within the definition of Church.

Contents

S**ection A – What this policy is for**

1. Policy statement

1.1 The Church is committed to protecting personal data and respecting the rights of all persons (**data subjects**) whose personal data is collected and used. Personal information is of significant value and this policy is designed to ensure that the Church complies with all relevant laws and adopts and maintains good practices.

The Church processes personal data to:

a) maintain a list of Church members, regular attenders and those enquiring about church activities. Data of minor children and those lacking capacity may be recorded with the consent of an appropriate adult or parent;

b) provide pastoral support for members and others connected with the Church;

c) provide services to the community;

d) maintain a record of those persons who are referred to other organisations;

e) safeguard young people and children and adults at risk;

f) recruit, support and manage staff and volunteers;

g) assist in applications for grants and other funding;

h) maintain accounts and records;

i) promote the Church's activities and services including activities with other denominations, faith groups and organisations;

j) maintain the security of property and premises;

k) respond effectively to enquirers and to handle any complaints;

l) monitor job opportunities for minority ethnic job seekers.

1.2 This policy sets out the legal obligations that apply whenever personal data is obtained, stored or used.

2. Why this policy is important

2.1 The Church recognises the harm and distress which misuse of personal data can cause and is committed to fulfilling its legal obligations to protect personal data from inaccuracy, misuse, or unauthorised dissemination, be that as a result of poor security or reckless/ careless disclosure or compilation.

2.2 This policy sets out the manner in which the obligations mentioned in paragraph 2.1 will be met both by the Church and by all individuals handling personal data.

2.3 In particular to comply with the legal requirements all personal data must be:

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.

Further restrictions apply in relation to the transfer of data outside the European Economic Area and if this is necessary reference should be made to the Data Protection Officer whose role is set out in paragraph below

3. Application of this policy

3.1 All trustees, employees, volunteers or other persons processing personal information on behalf of the Church are required to comply with this policy. In the event of any breach of this policy being recognised or suspected the Data Protection Officer must be notified immediately.

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

3.2 A leader or manager of any activity is required to ensure that in that activity any procedures that involve personal data follow the rules set out in this Data Protection Policy.

3.3 The Church will handle all personal information (including that pertaining to volunteers) in accordance with this policy.

3.4 Any appointed data processor/contractor appointed by the Church as a data processor is contractually required to comply with this policy. Any breach of the policy will be taken seriously and result in the institution of contract enforcement action against the company or the termination of the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (the Church) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

3.5 The Data Protection Officer [INSERT NAME] is primarily responsible for advising the Church and all trustees, employees and volunteers of their legal obligations under data protection legislation, monitoring compliance with that legislation, 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 him/her at [EMAIL ADDRESS].

3.6 All persons collecting or handling any personal data as part of their duties (paid or otherwise) for the Church must read this policy carefully and understand the obligations placed upon them as well as the Church's responsibilities in such processing activities.

3.7 The Church's procedures will be in line with the requirements of this policy but any concerns that such procedures might breach this policy should be raised with the Data Protection Officer.

4. Training and guidance

4.1 Periodically the Church will provide general training for all staff to raise awareness of their obligations and responsibilities, as well as to outline the law.

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

4.3 Managers and leaders must ensure that local volunteers receive adequate instruction in the implications of this policy for their working practises.

Section B – The church's data protection responsibilities

5. What personal information is processed?

5.1 In the course of the Church's activities information (personal data) may be collected and processed about many different people (data subjects). This includes data received directly from the person it is about, for example, where they complete forms or otherwise contact the Church. Information about data subjects may also be received from other sources including, for example, previous employers, doctors' surgeries, churches and relatives and where appropriate DBS checks.

5.2 The Church will process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data so received and processed can include information such as names and contact details, education or employment details, qualifications and visual images.

5.3 The Church may 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; criminal records, sexual life and sexual orientation.

5.4 Other data may also be considered 'sensitive' such as bank details, but will not be subject to the same legal protection as the types of data listed above.

6. Making sure processing is fair and lawful

6.1 Processing of personal data will only be fair and lawful when the purpose for the processing meets one or more of the legal basis in paragraph 6.2, and when the processing is transparent. This means that individuals will be provided with an explanation of how and why their personal data is processed at the point when that data is collected, as well as when data about them is received from other sources.

Use of personal data

6.2 Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

a) the processing is **necessary for a contract** with the data subject;

b) the processing is **necessary for us to comply with a legal obligation**;

c) the processing is necessary to protect someone's life (this is called "**vital interests**");

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

e) the processing is **necessary for legitimate interests** pursued by the Company 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**.

Use of 'special categories' of data?

6.3 Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

a) the processing is necessary for **carrying out our obligations under employment and social security and social protection law**;

b) the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;

c) the processing is carried out in the **course of our legitimate activities** and only relates to our members or persons we are in regular contact with in connection with our purposes;

d) the processing is necessary for **pursuing legal claims**.

e) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit consent**.

6.4 Before deciding which condition should be relied upon individuals should refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

Disclosure to individuals before use of their data

6.5 If personal data is collected directly from the individual they will be informed of:-

a) the existence and identity of the Church and contact details

b) the identity and contact details of the Data Protection Officer;

c) the reasons and legal basis for processing;

d) explaining the Church's legitimate interests;

e) Any consequences (where relevant) of not providing data needed for a contract or statutory requirement;

f) The identity of any person or organisation with whom we will share the data, and in particular if that includes disclosure 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' and will be given at the time when the personal data is collected.

6.6 If data is collected from another source, rather than directly from the data subject the data subject will be provided with the information described in section 6:5 as well as the categories of the data concerned and the source of the data.

This information will be provided to the individual in writing and no later than **1 month** after the data is received, unless a legal exemption under the GDPR applies. If the data is used to communicate with the data subject this information will be provided at the time of the first communication.

If the data is to be disclosed to another organisation or individual outside the Church in accordance with paragraphs 6:3 or 6:4 above, the data subject of this information will be provided with this information prior to disclosure occurring.

7. Consent to process data

7.1 Where none of the legal conditions set out in paragraphs 6:2 or 6:3 above apply the consent of the data subject to processing is required. The data subject must be advised as to the reasons why the consent is sought, including why the data is required and how it will be used. Consent will be specific to each process and will only be sought when the data subject has a real choice whether or not to provide their data.

7.2 Consent can be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

8. Processing for specified purposes

8.1 Personal data will only be processed for the specific purposes explained in the privacy notices (as described above in paragraph 6:5) or for other purposes specifically permitted by law. Those other purposes will be explained to data subjects in the way described in paragraph 6:5, unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and not excessive

9.1 Data will be collected and used only for, and to the extent required by, the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more information than is needed to achieve those purposes and in particular no data should be collected on the basis that it might be useful in the future.

10. Accurate data

10.1 Personal data held must be accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

11. Retention of data

11.1 Personal data must be retained no longer than is necessary for the purposes for which it was collected. The Data Protection Officer will advise processors of any guidance issued about retention+

11.2 Information on the retention of records can be found in Schedule 3.

12. Security of personal data

12.1 Appropriate measures will be used to keep personal data secure at all stages of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

12.2 Security measures are in place which will provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate the Company will take into account the following, and anything else that is relevant:

a) the quality of the security measure;

b) the costs of implementation;

c) the nature, scope, context and purpose of processing;

d) the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;

e) the risk which could result from a data breach.

12.3 Measures may include:

a) technical systems security;

b) measures to restrict or minimise access to data;

c) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;

d) physical security of information and of our premises;

e) organisational measures, including policies, procedures, training and audits;

f) regular testing and evaluating of the effectiveness of security measures.

It is incumbent on all persons having access to personal data to seek to apply these principles in their handling of such information and in the application of the security procedures set out in schedule 4.

13. Keeping records of data processing

13.1 To fulfil the Church's legal requirements clear records of all processing activities will be maintained including the reasons for decisions concerning personal data.

Section C – Working with data subjects

14. Data subjects' rights

14.1 All personal data will be processed in a manner which is compatible with the data subjects' rights, including their right to:

a) request access to any of their personal data (known as a Subject Access Request);

b) require the correction of inaccurate personal data;

c) restrict processing in certain circumstances;

d) object to processing in certain circumstances, including preventing the use of their data for direct marketing;

e) data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

f) not be subject to automated decisions, in certain circumstances; and

g) withdraw consent when such consent is relied on in connection with the processing of data.

14.2 A data subject can always request access to his or her file and if such a request is made in person it should be complied with in the manner set out in Schedule 4. If a written request is made by a data subject that relates or could relate to their data protection rights this must forwarded to the Data Protection Officer **immediately**.

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

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

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

15. Direct marketing

15.1 The Church 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 relating to **direct marketing**. This includes, but is not limited to, contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

> **Direct marketing** means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

15.2 Any direct marketing material that we send will identify the Church as the sender and will describe how recipients can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing they will cease to be the subject of such contact as soon as possible.

Section D – working with other organisations & transferring data

16. Sharing information with other organisations

16.1 The Church will only share personal data with other organisations or people when there is a legal basis to do so and when the data subject is aware of 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 are allowed to share personal data.

16.2 Records of information shared with a third party will be maintained, and such records will include recording any exemptions which have been applied, and why they have been applied. The Church will adhere to the ICO's statutory ***Data Sharing Code of Practice*** (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

17. Data processors

17.1 Before appointing a contractor who will process personal data on the Church's behalf (a data processor) due diligence checks will be conducted. 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. The Church will only appoint data processors who can provide us with sufficient guarantees that this will occur.

17.2 Data processors will be appointed on the basis of a written contract that will require the processor to comply with all relevant legal requirements and throughout the duration of the contract to be subject to performance monitoring and compliance with relevant legislation.

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

18.1 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.

18.2 Data will only be transferred outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

Section E – Managing change & risks

19. Data protection impact assessments

19.1 When it is proposed to carry out any data processing which is likely to result in a high risk a Data Protection Impact Assessment (DPIA) will be conducted. These include situations requiring the process of 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.

19.2 A DPIA will be conducted in other cases when it is appropriate to do so. If it is not possible to mitigate the identified risks such that a high risk remains the advice of the ICO will be sought.

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

20. Dealing with data protection breaches

20.1 Where staff or volunteers, or contractors working for us, think that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to the Data Protection Officer.

20.2 Records will be maintained of all personal data breaches, even if it is not necessary to report them to the ICO.

20.3 All data breaches which are likely to result in a risk to any person will be reported to the ICO. Reports will be made to the ICO within **72 hours** from when a trustee, volunteer, or employee becomes aware of the breach.

20.4 In situations where a personal data breach causes a high risk to any person, the Data Protection Officer will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay.

This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Schedule 1 – Definitions and useful terms

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

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.

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. 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 the Company holds 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 the Church is likely to hold personal data about include:

a) Church members
b) the people we care for and support;
c) employees (and former employees);
d) consultants/individuals who are the Company contractors or employees working for them;
e) volunteers;
f) tenants;
g) trustees;
h) complainants;
i) supporters;
j) enquirers;
k) friends and family;
l) advisers and representatives of other organisations.

ICO means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that compliance with legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

GDPR means General Data Protection Regulations introduced to unify and strengthen data protection for individuals.

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 their data is processed 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:

m) Racial or ethnic origin;
n) Political opinions;
o) Religious or similar (e.g. philosophical) beliefs;
p) Trade union membership;
q) Health (including physical and mental health, and the provision of health care services);
r) Genetic data;
s) Biometric data;
t) Sexual life and sexual orientation.

Schedule 2 – ICO Registration

Data Controller: The Leadership Team

Registration Number: ZA424063

Date Registered: 11th June 2018

Address:

Minehead Baptist Church
Parks Lane
Minehead
TA24 8BS

Schedule 3 – Disclosure

A client has an absolute right to disclosure of the information held about him or her. Disclosure of that information should be completed as quickly as possible following a request as failure to do so will cause a loss of good will and may result in a complaint.

Routine disclosure

This occurs during the course of the contact between the Church and the data subject ("the subject"). It is good practise to-

a) Take a photocopy of any original document produced by the subject and return the original;
b) Provide a copy of any document drafted during a meeting;
c) Provide a copy of any document subsequently received which relates to the subject. If this is forwarded by email a copy of the document and covering emails should be retained on the file.

Personal request

If an individual attends at the Church or other church premises and requests his/her file then-

a) The request should be attended to with the minimum delay;
b) The subject should be provided with the originals of any documents he has produced and copies retained
c) When the originals include audio or visual records these should be released without copying unless they constitute requests to the Church
d) The subject should be provided with the copies of any original documents which he has signed regarding his contact with the Church such as privacy notices and correspondence from him/her. Originals of these documents should be retained.
e) Copies of any documents relating to the subject and prepared by third parties addressed to the Church should be provided but the originals should be retained.

Request by email, letter or telephone

If such a request is made then-

a) The data subject should be advised immediately that the file will be transferred to the DPO;
b) The relevant leader/ manager should be advised of the request and arrangements made for the file to be despatched to the DPO.

Schedule 4 – security measures

The matters set out below are not designed to be an exhaustive listing of measures which should be taken to preserve the integrity and security of information received from data protection subjects (in this schedule referred to as subjects). There is an obligation on all persons dealing with such material to preserve it safely and securely and such preservations will depend on the factors in existence at any particular time. The following are therefore a list of the minimum criteria to be adopted.

Hard Copies

This section refers to physical documents not retained on a computer system such as paper records, photographs, recordings and handwritten notes. Such records are:-

a) Not to be removed from the location where they are stored;
b) When not in use to be retained in a locked filing cabinet or other secure and locked system. The cabinet itself should be secure and in an area to which the public do not have access;
c) Never to be left in a position where another individual could have access to them;
d) Never to be destroyed other than in the course of authorised "weeding".

Electronic systems – Computers

The use of the word "computer" in this section includes any electronic device for the recording or creating of information and therefore includes devices such as "laptops", mobile phones and ipads

a) All computers should be password protected and the password should be changed on a monthly basis;
b) Nominated members of staff and employees should be provided with a laptop for use on Church business. Such equipment should be used for no other purpose and those issued with such laptops should never use personal computers for Church business;
c) No computer should be removed from the location where it is retained other than for authorised usage safekeeping or repair. When not in use smaller items should be stored in a locked filing cabinet in a secure area to which the public do not have access;
d) If any computer is removed as described in c) above it should never be left in an unattended motor vehicle
e) No device for the transmitting or receiving of information such as a CD or memory stick should be inserted in a computer without the approval of the relevant leader/manager;
f) Notwithstanding paragraph e) above no such device provided by a subject or belonging to a volunteer or employees should ever be inserted in a church computer, unless authorised;
g) Personal data retained on personal computers and relating to Church business should be deleted as soon as it is no longer required;
h) If computers are made available to subjects for the purposes of e.g. job searches those users must not be able to gain access to the files of other hub users;

No document or record retained on a computer should be deleted other than in the course of authorised "weeding".