The Baptist Union of Scotland

DATA PROTECTION POLICY

Adopted: 16 July 2020

We, The Baptist Union of Scotland ('BUS'), a charitable company limited by guarantee and having its registered office at 48 Speirs Wharf, Glasgow G4 9TH (Company Number: SC620266; Registered Scottish Charity Number: SC049047; and registered as data controller under ICO Registration Number: Z6393741) are committed to protecting all information that we handle about the people we connect with in any way. Our aim is to respect people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

The legislation mentioned in this policy is the UK General Data Protection Regulation ('UK GDPR') which forms part of the Data Protection Act 2018 ('DPA 2018') and includes any subsequent amendment or re-enactment of that legislation.

Contents

Section A : About this policy

1. What this policy is for

Policy statement

BUS is committed to protecting personal data and respecting the rights of our data subjects, i.e. the people whose personal data we collect and use ('data subjects'). 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:

- maintain our list of member churches and their officers;
- provide support to our member churches; the members of their congregations; and others connected with us from the wider Christian community and beyond;
- host events and provide training opportunities of interest to our member churches and the wider community;
- maintain our list of accredited and pre-accredited ministers;
- maintain our list of both Executive and Non Executive Directors who together form our Trustee Board ('Trustee Board'); members of BUS' Council ('Council members'); and members of any BUS committees, task groups or other groups directly set up and commissioned by or which are otherwise related directly to BUS ('committees and groups');
- recruit, support and manage staff and volunteers;
- undertake research;
- maintain our accounts and records;
- promote our services;
- maintain the security and physical integrity of our property and premises;
- respond effectively to enquirers and handle any complaints; and
- liaise with other denominations and other organisations.

This policy has been approved by the Trustee Board, who are responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules that apply whenever we obtain, store or use personal data.

2. Why this policy is important

We are committed to protecting personal data from being misused; getting into the wrong hands as a result of poor security; being shared carelessly; or being

inaccurate. We do this because we are very aware that people can be upset and possibly harmed if any of these things happen.

This policy sets out the measures we are committed to taking as an organisation and what we will do to ensure that we comply with the relevant legislation.

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

- processed lawfully, fairly and in a transparent manner;
- processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and, where necessary, up to date;
- not kept longer than necessary for the purposes for which it is being processed;
- processed in a secure manner, by using appropriate technical and organisational means;
- processed in keeping with the rights of data subjects regarding their personal data.

3. How this policy applies to you & what you need to know

As an *employee, Non Executive or Executive Director, Council member, member of one of our committees and groups or a volunteer* processing personal information on behalf of BUS: You are required to comply with this policy. If you think that you have accidentally breached this policy, it is important that you immediately contact our General Director, who is our Data Protection Lead ('DP Lead') or in his absence, one of the other Executive Directors of BUS, so that we can take swift action to try and limit the impact of the breach.

(Note: Any person mentioned in the above paragraph who breaches this Data Protection Policy may be subject to disciplinary action and where that individual has breached this policy intentionally, recklessly, or for personal benefit, they may also be liable to prosecution or to regulatory action).

Additionally, as an *Executive Director of BUS*: You are required to make sure that any procedures involving personal data used in your area(s) of responsibility follow the rules set out in this Data Protection Policy.

As *data subjects of BUS:* BUS will handle your personal information in line with the terms of this policy.

As an *appointed data processor/contractor of BUS* (Note: This refers to any company, firm or individual appointed by us as a data processor): You are required to comply with this policy under the terms of your contract with us. Any breach of this policy will be taken seriously and could lead to us taking contract enforcement action against you or terminating our contract with you. Data processors have direct obligations under the GDPR UK primarily to only process data on instructions from us as the data controller and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

As stated above our DP Lead is our General Director and he is responsible for advising BUS and its Trustee Board, Council members, employees, members of groups and committees and volunteers about:

- their legal obligations under Data Protection law;
- compliance with Data Protection law and the ongoing monitoring of that compliance;
- data security breaches; and
- the development of this policy.

Any questions about this policy or any concerns that this policy has not been followed should be referred to our DP Lead at martin@scottishbaptist.org.uk or by writing to the BUS office at the address above.

Before you collect or handle any personal data as part of your work (paid or otherwise) for BUS, it is important that you take the time to read this policy carefully and understand both what is required of you and our responsibilities as an organisation when we process data.

Our procedures will be in line with the requirements of this policy, but if you are unsure or concerned about whether anything you plan to do, or are currently doing, might breach this policy, you must first speak to our DP Lead.

4. Training and guidance

We will provide general training at least annually for all staff and volunteers in order to raise awareness of their obligations and our responsibilities, as well as to outline the law.

We may also issue procedures, guidance or instructions from time to time. The staff team must set aside time for the whole team to look together at the implications for their work.

Section B : Our data protection responsibilities

5. What personal information do we process?

In the course of our work, we may collect and process information ('personal data') about many different people ('data subjects'). This includes data we receive direct from the person it is about, e.g. when they complete forms or contact us. We may also receive information about data subjects from other sources including, e.g. from previous employers and members/ officers of our member churches.

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, references for and visual images of people.

In many instances, we hold types of personal data that are called "special category data' under UK GDPR. This type of personal data can only be processed under strict conditions.

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is an overarching safeguarding requirement to process such data for the protection of children and adults who may be put at risk in our member churches. This processing will only ever be carried out on advice from our General Director as our Safeguarding contact person or his deputy, in his absence.

6. Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below; is necessary; 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 their data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

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

- the processing is done for a specific purpose with the clear consent of the data subject;
- the processing is necessary for a contract with the data subject;

- the processing is necessary for us to comply with a legal obligation;
- the processing is necessary to protect someone's life (this is called "vital interests");
- the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
- the processing is necessary for legitimate interests pursued by BUS or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

In BUS, the most used legal bases for processing are consent, contract and legitimate interests. There can be more than one of these legal bases used at a time, but whatever basis or bases are used, they must be specified in the appropriate privacy notice given to the data subjects concerned before processing their data.

How can we legally use special category data?

Processing of special category data is only lawful when, in addition to the legal basis or bases mentioned above, one of the extra conditions, as listed in Article 9 of the UK GDPR, is met. These conditions are as follows:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law)

In BUS, the conditions for use of special category data most usually relied upon will be because either the data subject has given explicit consent; because BUS is a not for profit organisation; or because the data is being processed for the purpose of archiving.

However, before deciding which of the 10 conditions outlined above should be relied upon at any given time, we may refer to the original text of the UK GDPR, as well as any relevant guidance and we will seek legal advice as required.

What must we tell individuals before we use their data?

If personal data is collected directly from the individual, we will inform them in writing about:

- our identity/contact details and those of the DP Lead;
- the reasons for processing, and the legal bases, explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement;
- who we will share the data with;
- if we plan to send the data outside of the UK;
- how long the data will be stored; and
- the data subjects' rights.

(Note: This information will usually be sent in the form of a document known as a privacy notice. This information will be given at the time when the personal data is collected).

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described in the bullet points immediately 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 1 month after we receive the data, unless a legal exemption under the UK 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 on to someone else outside of BUS, we will only do so provided (a) that is a lawful action to take; and (b) we have first given the data subject this information before we pass it on..

7. When we need consent to process data

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 for which we are requesting consent and we will only ask for consent when the data subject has a real choice as to whether or not to provide us with their data.

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

8. Processing for specified purposes

We will only process personal data for the specific purposes explained in our privacy notices or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described at paragraph 6 above, unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and not excessive

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 the relevant privacy notice). We will not collect more than is needed to achieve those purposes. We will not collect any personal data “just in case” we want to process it later.

10. Accurate data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

11. Keeping data and destroying it

We will not keep personal data longer than is necessary for the purposes for which it was collected. We will comply with any official guidance issued to our sector about retention periods for specific records.

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

12. Security of personal data

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

We will implement security measures which 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 we will take into account the following, and anything else that is relevant:

- the quality of the security measure;
- the costs of implementation;
- the nature, scope, context and purpose of processing;
- the risk (of varying likelihood and severity) to the rights and freedoms of data subjects; and
- the risk which could result from a data breach.

Measures may include:

- technical systems security;
- measures to restrict or minimise access to data;
- measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- physical security of information and of our premises;
- organisational measures, including policies, procedures, training and audits;
- regular testing and evaluation of the effectiveness of security measures.

13. Keeping records of our data processing

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 about whom we process data (data subjects)

14. Data subjects' rights

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

- request access to any of their personal data held by us (known as a subject access request);
- ask to have inaccurate personal data changed;
- restrict processing in certain circumstances;
- object to processing in certain circumstances, including preventing the use of their data for direct marketing;
- 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;
- not be subject to automated decisions in certain circumstances; and
- withdraw consent when we are relying on consent to process their data..

If an employee of BUS, member of the Trustee Board, Council member, member of any of our groups and committees or a volunteer receives any request from a data subject that relates (or could relate) to their data protection rights, this will be forwarded to our DP Lead immediately.

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 timescale can be extended by up to two months in some circumstances.

All data subjects' rights are provided free of charge. Any information provided to data subjects will be concise and transparent, using clear and plain language.

15. Direct marketing

We will comply with the rules set out in the UK GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around direct marketing. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging and telephone (both live and recorded calls).

Any direct marketing material that we send will identify BUS as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

Section D : working with other organisations & transferring data

16. Sharing information with other organisations

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 are allowed to share personal data.

We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO's Code of Practice on Data Sharing (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

17. Data processors

When appointing a contractor who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

We will only appoint data processors on the basis of a written contract which will require the processor to comply with all relevant legal requirements. Throughout the term of any such contract, we will continue to monitor the data processing and the processor's compliance with the contractual terms..

18. Storage of personal data outside the UK

Personal data may be stored outside the UK but only in compliance with UK GDPR and only with data processors duly appointed by BUS.

Section E – Managing change & risks

19. Data protection impact assessments

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). This will include situations when we process data relating to vulnerable people; trawling of data from public profiles; using new technology; and transferring data outside the UK. Any decision not to conduct a DPIA will be recorded.

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.

DPIAs will be conducted in accordance with the relevant ICO Code of Practice.

20. Dealing with data protection breaches

Where an employee, member of our Trustee Board, Council member, member of any of our groups and committees, a volunteer, a data processor or other contractor working for us thinks that this policy has not been followed; that data security might have been breached; or that data may have been lost, this will be reported immediately to our DP Lead in accordance with our Data Breach Procedure.

We will keep records of personal data breaches, even when the breach does not require to be reported to the ICO.

We will report to the ICO on all data breaches which are likely to result in a risk to any person. Reports will be made to the ICO within 72 hours from when someone within BUS becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform the data subjects whose information is affected without undue delay. This can include situations where, for example, bank account details are disclosed or 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 UK GDPR. The UK 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. BUS is the data controller of the data which we process.

data processors include any individuals (but not employees) or organisations, which process personal data on our behalf and on our instructions.

data subjects include all living individuals about whom we hold or otherwise process their personal data. 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 about whom we are likely to hold personal data include:

- members of our Trustee Board, Council members and members of any of our groups or committees;
- our employees (and former employees);
- our ministers and those applying to our Board of Ministry
- consultants/individuals who are our contractors or employees working for them;
- our volunteers;
- complainants (if any);
- supporters;
- enquirers;
- advisers and representatives of other organisations.

ICO means the Information Commissioner's Office, which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action when 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, deleting 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 category data (as identified in the UK 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.

Schedule 2 – ICO Registration

Data Controller: The Baptist Union of Scotland

Registration Number: Z6393741

Date Registered: 1/3/2002 and renews annually

Address: 48 Speirs Wharf, Glasgow G4 9TH