Bunyan Baptist Church
Stevenage

Refreshing community for everyone

Data Protection

Policy

3rd Edition – GDPR compliance

Policy history

Policy author	**Eric Beach**
Replaces	**2nd Edition dated 18 March 2014 and reviewed in April 2017**
Date of first draft	**April 2018**
3rd Edition Approved	**To be approved at Church Meeting – 19th June 2018**
Review Date	**Three years after approval**

This policy should be operated with reference to the BUGB guidance document L13 Data Protection (March 18 edition) available at
https://www.baptist.org.uk/Groups/302154/Data_Protection_and.aspx?redirected=1

Bunyan Baptist Church
DATA PROTECTION POLICY

Introduction

The need for Data Protection legislation arose because of the growing use of computers which can store a vast amount of information about individuals. Without safeguards these personal details could easily be accessed by individuals, organisations and the Government. The Data Protection Act 1998 sought to protect an individual against the unfair use of personal information. This is being updated in the form of the *General Data Protection Regulations [GDPR]* which come into effect on 25th May 2018.

Bunyan Baptist Church is committed to protecting personal data and respecting the rights of our **data subjects**; the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

a) maintain our list of church members [and regular attenders];
b) provide pastoral support for members and others connected with our church;
c) provide services to the community including [Toddler Group, Foodbank];
d) safeguard children, young people and adults at risk;
e) recruit, support and manage staff and volunteers;
f) maintain our accounts and records;
g) promote our services and other activities;
h) respond effectively to enquirers and handle any complaints and
i) serve our charitable purposes.

We have purchased a licence for using Church Suite (https://churchsuite.com/) and it has been decided that all such data collected should be stored on this web-based GDPR compliant database. Anyone working for or providing services / running groups for the church should use this for storing any collected data. They should not retain any information on their own computer or within their own home.

This will allow the trustees to identify what data is held and processed by the church and control the use and storage of that data. In this way we should be able to ensure that we adhere to the data protection principals outlined below.

This policy has been approved by the church's Charity Trustees 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.

The Basics

Data protection law covers information held by any person, business or organisation about a living individual. Under the new regulations, this will apply to information kept on computers as well as paper records that are catalogued in such a way as to allow data about individuals to be easily retrieved. There are one or two exceptions. For example, information held for purely private and domestic purposes is not covered, so your own address book with your friends' names and addresses will not be subject to the law. Apart from these limited exceptions, the law applies to all personal data held by anyone. It therefore applies to all such information held by churches and church groups and those holding that data on behalf of churches.

The law does not only apply to secret, confidential or sensitive information.

For example, the church directory will be considered to contain personal data and so is covered by GDPR. The details of church members who give charitable donations under the Gift Aid scheme, and the details of individual missionaries or other beneficiaries who benefit from those donations, will be covered by the Regulations, as will details of church staff (such as payroll details and comments contained in employment records). Confidential details of discussions about pastoral issues contained in sets of minutes would also be covered.

All this means that it is simply impossible for a church or church group to operate at all without needing to comply with the GDPR.

Breaching confidentiality of people's records in not acceptable and doing so will severely damage the reputation of the church and should it constitute a breach of the General Data Protection Regulations could result in a criminal prosecution.

What can I do to comply with this policy?

1. If you collect information about people for church business then this must be stored on the Church Suite database. You should not keep the data on your own computer/device or in paper form unless specifically authorised by the Trustees [eg child health data which might be needed in an emergency during a residential weekend away]

2. If you think it is necessary to collect personal data you should first check with the Trustees to see whether it is acceptable or necessary

3. When collecting data you must make sure that the person whose data you are collecting is aware that you are doing it, knows exactly why you are doing it and has consented to you holding a using their data. A written privacy notice and consent form will be required for this.

4. If authorised to keep that information by the Trustees, make sure the information lines up with the eight data protection principals below. If in doubt, ask a Trustee!

5. Make sure that your computer [or any other electronic device that you use to access that data – eg phone, tablet etc] is password protected, especially if you take it out of the house.

6. Make sure that your computer / device has adequate anti-virus software that is up to date and working properly to stop your machine being hacked and the information stolen

7. If you need help with your computer / device to make sure it is secure, then ask the Trustees. We have some who are very computer literate!

Bunyan Baptist Church is committed to protecting personal data and respecting the rights of our data subjects; the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We process personal data to help us:

a) maintain our list of church members [and regular attenders];
b) provide pastoral support for members and others connected with our church;
c) provide services to the community including [Twinklers];
d) safeguard children, young people and adults at risk;
e) recruit, support and manage staff and volunteers;
f) maintain our accounts and records;
g) promote our services and events etc;
h) serve our charitable purposes.

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

If you are an employee, trustee or volunteer processing personal information on behalf of the church, you are required to comply with this policy.

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

Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you must first speak to the Data Protection Officer / Senior Minister. If you think that you have accidentally breached the policy it is important that you contact our Data Protection Officer / Senior Minister immediately so that we can take swift action to try and limit the impact of the breach.

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.

You will be expected to attend Data Protection training at least once every two years to raise awareness of your obligations and our responsibilities, as well as to outline the law. We may also issue procedures, guidance or instructions from time to time. [Managers / team leaders must set aside time for their team to look together at the implications for their work.]

If you are a team leader you are required to make sure that any procedures that involve personal data, that you are responsible for in your area, follow the rules set out in this Policy.

If you are a data subject of Bunyan Baptist Church, we will handle your personal information in line with this policy.

Our Data Protection Officer / Senior Minister is responsible for advising the trustees, staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at andrew@bunyan.org.uk

Eight Principles

There are eight principles which must be complied with whenever personal data is processed. These were laid out in the original Data Protection Act and are also the basis of GDPR.

- The data must be processed fairly and lawfully.

- The data must be obtained only for specified lawful purposes and cannot be used for other purposes.

- The data must be relevant and not excessive. For example, you do not need assessments of someone's income for a membership list.

- The data must be accurate and kept up to date. This will involve having some practice in place to review and update data; this will need to be appropriate given the nature of the data and the purposes for which it is held.

- The data must not be kept for longer than is necessary. This means that data held on Church Suite must be regularly reviewed and deleted when it is no longer necessary.

- The data must be used in accordance with the rights of the individual concerned. For example, the individual has a right under GDPR to access to copies of his or her personal data. Using Church Suite will ensure that all data about an individual is held in one place and that we will be able to identify how it has been processed. If an individual wants a copy we will be able to pull up the record easily. This also means that you shouldn't write anything about someone in notes, minutes etc that you would not feel comfortable to share with them or allow them to read.

- The data must be kept secure. This means there should be both technical measures (eg ensuring that the computers used by Trustees etc have passwords and firewalls to prevent the wrong people accessing them) and physical measures (eg paper records should not be treated casually but stored in 'locked' environments) which are appropriate given the nature and importance of the personal data.

- The data must not be transferred overseas, except to countries in the European Union and EEA and some other specified countries. The use of Church Suite to hold the data will ensure that this does not occur.

The Technical Terms

Like all specialist subjects there are some technical terms to be understood. These are the most important ones.

Data subject refers to the individual whose personal data you hold. In a typical church situation this would be church members, members of the congregation, children in the Sunday School or Youth Group, those attending Christianity Explored courses etc whose names and personal details are recorded.

Personal data means information relating to a living individual who can be identified from that data (or from that data plus other information in your possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal) or a statement of intention about them.

Sensitive Personal Data [also referred to in the GDPR as **'Special categories' of data**] is personal data which consists of information concerning the data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a Trade Union, physical or mental health condition, sexual life, commission or alleged commission of any offence, a record of any proceedings for any offence committed or alleged, or a record of any sentence or proceedings. Much of the information which churches are likely to process will be sensitive personal data as it is likely to concern the data subject's religious beliefs. **This personal data can only be processed under strict conditions. [NB** *We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is an overarching safeguarding requirement to process this data for the protection of children and adults who may be put at risk in our church. This processing will only ever be carried out on advice from the Ministries Team of the Baptist Union of Great Britain or our Regional Association Safeguarding contact person.*]

Data classes define the type of personal data that is being processed. Normally a church will only hold personal data which falls in the 'Personal Details' class. If this is the case, then churches may not need to notify (register with) the Information Commissioner's Office.

Data controller refers to the person or persons who determine the purpose and the manner by which personal data is to be processed. In the case of a Baptist church, the data controller will usually be the Charity Trustees (usually the minister, deacons and elders or Leadership Team). Please note however that if the minister maintains personal data separately (not under the overall direction of the Charity Trustees) then the Minister should notify the ICO as he or she will be the data controller and will not have the benefit of the exemption provisions set out below.

Data processor refers to the person who actually processes the personal data on behalf of the data controller. There will be several people who are actually processing personal data and they are responsible to the Charity Trustees as the data controller. Examples of data processors might be the Church Treasurer or Child Protection Administrator.

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.

Registration

Many organisations that hold and process personal data are required to be registered with the Data Protection Registrar. However, The Government have recognised that, for many organisations, compulsory registration with the Data Protection Registrar, is not necessary.

Churches, if they are processing personal data for usual church purposes, may not need to notify the Data Protection Registrar. However, the Baptist Union has recommended that churches do register 'just in case'. This will cost the church about £40 a year. It is therefore something that Bunyan Baptist Church will do.

Privacy Notices

If personal data is collected directly from the individual, we will inform them at the time the data is collected [in writing – a document commonly known as a 'Privacy Notice'] about;

- our identity/contact details [and those of the Data Protection Trustee],
- the reasons for processing, and the legal bases, [including explaining any automated decision making or profiling], 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 and if we plan to send the data outside of the European Union;
- the use of Church Suite as our electronic data storage mechanism;
- how long the data will be stored and
- the data subjects' rights.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described above as well as

- the categories of the data concerned and
- the source of the data.

This information will be provided to the individual in writing and no later than within **1 month** after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Bunyan Baptist Church, we will give the data subject this information before we pass on the data [unless the reason for passing it on is to prevent a crime or harm to the data subject or others and telling them would mean that the crime / harm could not be prevented].

The privacy notice should also outline the data subject's rights which include the right to

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

b) ask to have inaccurate personal data changed;

c) restrict processing, in certain circumstances;

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

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

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

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

It should inform them that if a request is received from a them [as the data subject], then this will be passed on to the lead minister as soon as possible and that we will act on any valid request within at least **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. We will provide this service free of charge and provide all information in a concise and transparent format using clear and plain language.

Consent

Where none of the other legal conditions apply to the processing, we are required to get consent from the data subject. We will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

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.

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 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 Bunyan Baptist Church or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

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

How can we legally use 'special categories' of data?

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:

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

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

Email prayer chain message

No-one's name [or data that identifies someone] should be included within a church prayer chain message without their consent. Generally, we would expect anyone that we are asked to pray for to have agreed that their details and prayer needs can be shared with the congregation [as a matter of pastoral sensitivity if not as part of the data protection legislation]. Where a member asks us to pray for one of their relatives, we should check that they have asked their relative [a] if they can be named for this purpose and [b] that they are happy for you to release the information you are passing on to a group of people who they may not know.

Videoing / photographing of services, events etc

Where this is being done for 'publication' [eg on a website, social media etc], care must be taken to ensure that those who are appearing in the video are happy for it to be put into the public domain. If a service or event is to be recorded for such reasons then individuals coming to the event should be given as much notice as possible and there should be an area of the church / venue where people who don't wish to be shown can sit such that they are hidden from the camera. Photographs of events such as 'Big Lunch' where members of the public are in attendance will need to be carefully vetted to ensure that only those who are happy for their image to appear will be shown.

Sermons published on websites etc as audio files

Where individuals are named within such audio recordings, consent must be obtained to ensure that they are happy that what has been said about them is published. If they are doing readings etc then they should be asked if they are happy to be named in the recording.

DBS Checks

When individuals engage in the DBS check they sign a consent form for the check to be completed and as such the process of doing these checks will be GDPR compliant. Holding and using the information that is returned to the church must be strictly controlled and the data only available to those who need to know for the purpose of safeguarding. The storage of that information must be robust so that the information cannot be leaked inadvertently.

Trustees / employees /volunteers leaving their post

Where someone stops working for the church, they should return to the church all records / data pertaining to their role and also delete any copies of that data that is held on computers [and other electronic devices] that they own. The only exception might be if they need to keep the data in case there is some sort of legal case against them. In this case the trustees should be notified and approval gained.

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

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 ICO's Code of Practice 'Conducting privacy impact assessments'.

Dealing with data protection breaches

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 / Senior Minister.

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

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

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Responsibilities

Trustees

The trustees [or their nominated representative] will carry out the role of Data Controller

Data Controller

The Data Controller will hold a register of the data collections made within the church where there is sensitive personal data – eg information over and above that which might normally be found in the Church Directory. This register will identify

- who is the primary holder of this data
- where / how the data is held [eg on a person's computer, in a book, paper records etc]
- what categories of information are being held about people

The Trustees should ensure that these data sets fall within the *exempt purpose* and that it is lawful to hold them.

Elements of the register will be available for public consumption [ie on the church website as an appendix to this policy] so anyone involved with the church will know what sort of data is being held and who holds it. This will allow individuals to check if their data is correct and up to date.

Data Processors

Anyone who collects data sets for church purposes must ensure that the nature of the data held is in the register held by the data controller.

Data processors may not pass information on to other people unless they have the consent of the person who the information concerns.

Data processors have a duty to ensure that the information held is within the exemption guidelines above and only consists of the elements noted in the register. If there is concern that it may fall outside the *exempt purpose* then the data processors must seek advice from the Data Protection Officer / Senior Minister as to whether it is acceptable to hold this data. This may be the case if counselling notes etc are held. Data that falls outside of these boundaries may only be held with the express written permission of the data controller / trustees.

Data processors have a responsibility to ensure that any data is securely held. Loss of data should be reported to the data controller. If the data processors has the information on a computer that is disposed of, then proper steps should be taken to ensure that the data is erased from the machine. If the machine works when disposed of then the recovery disk should be used to permanently erase all data from the hard drive before it is passed on. If it has failed and cannot be repaired then the hard drive should be removed and either retained or destroyed in such as way as to make the data irretrievable. Old paper records should be shredded.