Bishopdown Evangelical Church

Bishopdown Road

Salisbury

SP1 3DU

DATA PROTECTION POLICY

Adopted: 24th April 2018

Reviewed November 2021

Next Review due November 2022

Bishopdown Evangelical Church (BEC) is committed to protecting all information that we handle about people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

Contents…….. 2

Section A – Legislation

The need for legislation covering Data Protection arose because of the growing use of computers which can store a vast amount of personal information about individuals. Without safeguards these personal details could easily be accessed by individuals and other organisations.

The **Data Protection Act 1998** was introduced to protect individuals against the unfair use of their personal information. The 1998 Act was replaced by the **2018 Data Protection Act (DPA)** which incorporated the European General Data Protection Regulations (GDPR). When the UK left the European Union the GDPR remained part of UK Data Protection legislation in the form of the Retained General Data Protection Regulations (UK GDPR), but the UK government now has the independence to keep the data protection framework under review. There are a number of fundamental principles (the Data Protection Principles) which the original DPA established which are based upon the rights of the individual to respect for their private and family life, free from interference by the State (in turn based upon Article 8 of the European Convention on Human Rights). The principles are also incorporated in the 2018 Act.

These principles are based upon the right of an individual to know what data is being held about them and to check its accuracy; and the concept that someone's personal information should be used only for the specific purposes for which it is expressly held by an organisation and not disclosed to those who are not authorised to hold it.

If a church processes any personal data, it must follow the rules set out in the DPA. Failure to do so could result in enforcement action being taken, by the regulator, the Information Commissioner's Office (ICO), against the church in question or against the trustees if the church is unincorporated.

These seven principles of Data Protection should lie at the heart of your approach to processing personal data.

Lawfulness, fairness and transparency

This means that you will need to

- identify the lawful basis for collecting and using personal information
- ensure that you don't process the data in a way that is detrimental, unexpected or misleading to the individuals concerned
- be clear, open and honest with people about how you will use their personal information

Purpose Limitation

This means that you will need to be clear about what your purposes for processing personal information are.

Data Minimisation

This means that you need to make sure that the personal information you are processing is:

- **adequate** (sufficient to meet your stated purpose)
- **relevant** (has a clear and rational link to that purpose)
- **limited** to what is necessary (you don't hold more information than you need)

Accuracy

This means that you will need to:

- do what you can to ensure the information you hold is not incorrect or misleading
- take reasonable steps to correct or remove incorrect data as soon as possible

Storage Limitation

This means that you should not keep personal information for longer than you need to.
You will need to think about (and be able to justify) how long you keep personal information.

Integrity and confidentiality (security)

You must ensure that you have appropriate security measures in place to protect the personal information you hold.

Accountability

This principle requires you to take responsibility for what you do with personal information and how you comply with the other principles. You therefore need to have appropriate measures and records in place to demonstrate your compliance.

Section B - What this policy is for?

1. Policy statement

1.1 Bishopdown Evangelical 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, but not limited to, Parent & Toddler Group, Children's clubs, Tuesday Lunch.

d) safeguard children, young people and adults at risk.

e) recruit, support and manage staff and volunteers.

f) maintain our accounts and records.

g) respond effectively to enquirers and handle any complaints

1.2 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.

2. Why this policy is important

2.1 We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

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

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

a) processed **lawfully, fairly and in a transparent manner**.

b) processed for **specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes.

c) **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed.

d) **accurate** and, where necessary, up to date.

e) **not kept longer than necessary** for the purposes for which it is being processed.

f) processed in a **secure** manner, by using appropriate technical and organisational means.

g) processed in keeping with the **rights of data subjects** regarding their personal data.

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

3.1 **As an employee, trustee, member or volunteer** processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy, it is important that you contact our Data Protection Officer 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.

3.2 **As an employee, trustee, member or volunteer:** You are required to make sure that for any procedures that involve personal data, that you are responsible for in your area, you follow the rules set out in this Data Protection Policy.

3.3 **As a data subject of Bishopdown Evangelical Church:** We will handle your personal information in line with this policy.

3.4 **Our Data Protection Officer** is responsible for advising BEC and its 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 admin@bishopdownevangelicalchurch.org.uk

3.5 Before you collect or handle any personal data as part of your work (paid or otherwise) for BEC 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.

3.6 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.

4. Training and guidance

4.1 We will provide training for new workers as required. The policy will be reviewed annually at a Church Members meeting and all relevant members who hold data will be required to read and sign the policy updates to raise awareness of their obligations and our responsibilities.

Section C - Our data protection responsibilities

5. What personal information do we process?

5.1 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 straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers.

5.2 We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details, donor's information, and visual images of people.

5.3 In some cases, we hold types of information that are called **"special categories"** of data in the GDPR. This personal data can only be processed under strict conditions.

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

5.4 We will not hold information relating to criminal proceedings or offences or allegations of offences.

5.5 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 a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

How can we legally use personal data?

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 BEC 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?

6.3 Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, extra conditions are met. These conditions include where:

a) that the processing is carried out as part of the **legitimate activities of a non-profit body** or association which exists for religious purposes and where the processing: − is carried out with the appropriate safeguards for the rights and freedoms of data subjects

b) **Necessary to fulfil an employment law obligation**: this will be relevant in relation to the sensitive personal data of employees of the church which are processed in connection with their employment e.g., to maintain records in relation to statutory sick pay.

c) **Necessary to protect the vital interests of the data subject** or some other person (where their consent cannot be obtained) – applies in 'life or death' situations.

d) **Necessary for legal advice/proceedings** e.g., this may apply where the church needs to obtain legal advice e.g., where the church faces possible or actual legal action by a member or employee and these individuals' sensitive personal data need to be shared with a solicitor or barrister in order to obtain legal advice.

e) **For ethnic monitoring/equal opportunities processing**

In many cases, therefore, the processing carried out by the church may not be based upon the data subject's consent but can be done lawfully using one of the grounds listed above.

f) 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, we may refer to the current text of the GDPR as well as any relevant guidance and seek legal advice as required.

What must we tell individuals before we use their data?

6.5 If personal data is collected directly from the individual, we will inform them about; our identity/contact details and those of the Data Protection Officer, 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.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

If we have any need to pass the data onto someone else outside of BEC we will give the data subject this information before we pass on the data.

7. When we need consent to process data

7.1 Under the UK GDPR, consent is clearly defined as being quite explicit and fully informed, unambiguous, involving some kind of positive step on the part of a data subject (e.g., by ticking a box, returning a signed form or by clicking through a carefully and specifically worded consent statement on a website). It is clear that there is no room for implied consent. In addition, the UK GDPR makes it quite clear that consent must be very easy to withdraw at any time without detriment to the data subject.

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

7.3 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

8.1 We will only process personal data for the specific purposes explained in our privacy notices (as described above in Section 6.5) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described in Section 6 unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and not excessive

9.1 We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data "just in case" we want to process it later.

10. Accurate data

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

11. Keeping data and destroying it

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

11.2 Information about how long we will keep records for can be found in our Data Retention Schedule (Schedule 2).

12. Security of personal data

12.1 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.

12.2 We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

12.3 Where data is stored electronically it will be on devices that are password protected. Where data is stored physically it will be kept in a locked drawer or cupboard.

13. Keeping records of our data processing

13.1 To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

Section D - Working with people we process data about (data subjects)

14. Data subjects' rights

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

a) request only access to any of their own 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) withdraw consent when we are relying on consent to process their data.

14.2 If any of the church group leaders receive a request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Officer **immediately**.

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

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

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

15.2 Any 'direct marketing material' that we send will identify BEC 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 E - working with other organisations & transferring data

16. Sharing information with other organisations

16.1 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed staff or Trustees are allowed to share personal data.

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

Section F - Managing change & risks

17. Data protection impact assessments

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

18. Dealing with data protection breaches

18.1 Where staff or volunteers 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.

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

18.3 We will report all data breaches which are likely to result in a risk of adversely affecting an individual's rights and freedoms, to the ICO. Reports will be made to the ICO within **72 hours** from when someone in the church becomes aware of the breach.

18.4 In situations where a personal data breach causes a high risk of adversely affecting an individual's rights and freedoms, 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.

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. We are the data controller of data which we process.

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

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

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

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

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

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

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

a) Racial or ethnic origin.

b) Political opinions.

c) Religious or similar (e.g., philosophical) beliefs.

d) Trade union membership.

e) Health (including physical and mental health, and the provision of health care services).

f) Genetic data.

g) Biometric data.

h) Sexual life and sexual orientation

Schedule 2 **Data Retention Schedule**					
Section	**Group**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**
Information re Church Groups	Noah's Ark Data	Registration forms will be kept while children still attending the group and for up to 3 years after last contact in order to inform them of other groups.	Good Practice	Paper copies of registration forms completed by parents. Kept in locked drawer in leaders' home. Taken to the church premises during the group and kept secure during the group. Email addresses may also be held on password protected devices.	Destroy
	Lion's Club	Registration forms will be kept for at least 3 years after the form has been completed. They will also be kept while children are still attending the group and for up to 3 years after last contact in order to inform them of other groups or events.	BUGB guidelines Good Practice	Paper copies of registration form completed by parents. Kept in locked drawer in leaders' home. Taken to the church premises during the group and kept secure during the group. Email addresses may also be held on password protected electronic devices.	Destroy
	Kings Club	Registration forms will be kept for at least 3 years after the form has been completed. They will also be kept while children are still attending the group and for up to 3 years after last contact in order to inform them of other groups or events.	BUGB guidelines Good Practice	Paper copies of registration form completed by parents. Kept in locked drawer in leaders' home. Taken to the church premises during the group and kept secure during the group. Email addresses may also be held on password protected electronic devices.	Destroy
	Lighthouse	Registration forms will be kept for at least 3 years after the form has been completed. They will also be kept while children are still attending the group and for up to 3 years after last contact in order to inform them of other groups or events.	BUGB guidelines Good Practice	Paper copies of registration form completed by parents. Kept in locked drawer in leaders' home. Taken to the church premises during the group and kept secure during the group. Email addresses may also be held on password protected electronic devices.	Destroy
Section	**Group/ Documents**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**

Information re Church Groups continued	Holiday Club	Registration forms will be kept for at least 3 years after the form has been completed. They will also be kept while children are still attending the group and for up to 3 years after last contact in order to inform them of other groups or events.	BUGB guidelines Good Practice	Paper copies of registration form completed by parents. Kept in locked drawer in leaders' home. Taken to the church premises during the group and kept secure during the group. Email addresses may also be held on password protected electronic devices.	Destroy
	Tuesday Lunch	For one year after last contact	Good Practice	Electronic list of names and telephone numbers, which is printed and kept in a locked cupboard at the church building for emergency contact.	Destroy
Membership	Church Members List (Names)	Retained permanently but reviewed and updated regularly	Good Practice	Electronic list of members details held by Minister and Church Secretary. Password protected	To Archive if Church closes
	Church Address List – Contact details of Church Members and regular attenders	While a member or regular attender. List is reviewed annually, and names will be removed from list after one year of no contact or when leaves the church.	Good Practice	Electronic list held by Church Secretary. Paper copies given to each member on the list. At least one paper copy is held in locked cupboard at church premises for emergency contact	Destroy
	Pastoral Information	For one year after last contact. It is good practice to record pastoral visits or meetings, noting the date, time, location, subject and any actions which are to be taken. The record of these meetings should stick to facts and try to avoid opinion. Any records of safeguarding allegations, concerns or disclosures should be passed on to the Designated Person for Safeguarding and stored in a safe and secure manner for at least 75 years	Good Practice	Stored electronically in a password protected computer	Destroy Keep for 75 years
Section	**Documents**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**

Employment and HR	All information relating to recruitment, selection and development whilst in post	6 years after post-holder has left your employment	Limitation Act 1980[(1)]	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Information on any disciplinary or grievance matter that is still 'live' on the individual's personnel file, including information on any penalty or warning imposed	6 years after post-holder has left your employment	Limitation Act 1980[(1)]	Electronic and paper copies in locked drawer and password protected computer	Destroy
	Information on an individual's health and sickness record, including information on any adjustment made to their working pattern, either on a temporary or permanent basis	6 years after post-holder has left your employment	Limitation Act 1980[(1)]	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Redundancy records	6 years from date of redundancy	Limitation Act 1980[(1)]	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Information on any safeguarding concern or matter in which the employee was involved in any way	75 years after employment/role ceases	Requirements of the Independent Inquiry into Child Sexual Abuse (IICSA)	Electronic and/or paper copies in locked drawer and password protected computer	Not Applicable
	Parental leave records	18 years from the date of the birth of a child	To enable future employers to check entitlement	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Section	**Group**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**
Employment and HR continued.	Payroll Records including correspondence with HMRC	6 years from the end of the financial year the records relate to.	Charities Act and HMRC	Electronic records on password protected device and/or paper records in locked cupboard.	Destroy

	Pension Records	According to schedules set by the Pension Provider		Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Application forms and interview notes for unsuccessful candidate	6 moths – 1 year	2010 Equalities Act recommends 6 months. One year limitation for defamation actions under Limitations Act.	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Complaints Records	1 year where complaint referred elsewhere otherwise 6 years from last action	Limitation Act 1980	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Notes: [1] Six years is generally the time limit within which proceedings founded on contract may be brought					
	Application forms and interview notes for unsuccessful candidate	6 months to a year	2010 Equality Act recommends six months. One year limitation for defamation actions under Limitation Act.	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Complaints records	1 year where complaint referred elsewhere otherwise 6 years from last action. Limitation Act 1980	Limitation Act 1980	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Finance	All financial records – invoices, bills, bank statements, paying in books etc	6 years from the end of the financial year the record relates to	Charities Act and HMRC Rules	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Gift Aid declarations	6 years after the last payment was made	HMRC Rules	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Legacy information (i.e., documents which relate to a legacy received by the church)	6 years after the deceased's estate has been wound up	In line with requirements for other financial information	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Section	**Group**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**
Finance continued.	Church Annual Accounts and Reports	10 years [(2)]	Good practice	Electronic and/or paper copies in locked drawer and password protected computer	Archive (e.g., County Archive Office)
	Payroll records including correspondence with HMRC	6 years from the end of the financial year the records relate to.	Charities Act and HMRC Rules	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Notes [(2)] Theses should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the church before sent to archives.					

Health & Safety	Reportable accidents / accident book	3 years after date of entry or end of any investigation if later	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Records documenting external inspections	3 years after date of inspection	Good Practice	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Insurance	Public liability policies and certificates	**Permanently**	Historical Claims/ commercial practice	Store securely with electronic copy as backup	
	Employer's liability policies	**Permanently**	Employers' Liability (Compulsory Insurance) Regulations 1998 suggests 40 years	Store securely with electronic copy as backup	
	Sundry insurance policies and insurance schedules	Until claims under policy are barred or 6 years after policy lapses, whichever is longer	Commercial practice	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
	Claims correspondence	6 years after last action	Commercial practice	Electronic and/or paper copies in locked drawer and password protected computer	Destroy
Meetings	Church Meeting Minutes	10 years from the date of the meeting [(3)]	Good Practice	Electronic and/or paper copies in locked drawer and password protected computer	Archive (e.g., County Archive Office)
	Trustee Meeting Minutes	10 years from the date of the meeting [(3)]	Good Practice	Electronic and/or paper copies in locked drawer and password protected computer	Archive (e.g., County Archive Office)
Section	**Group**	**Documents retained for:**	**Reason**	**How data held and stored**	**Action after retention period**
Meetings continued	Minutes of internal groups	5 years from the date of the meeting	Good Practice	Electronic and/or paper copies in locked drawer and password protected computer	Destroy unless of particular value in which case send to Archive
Safeguarding	See Church Safeguarding Policy for information				
Notes [(3)] These should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the church before sent to archives.					

Schedule 3 – Privacy Notice

Privacy Notice

Bishopdown Evangelical 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.

Under UK General Data Protection legislation the church Charity Trustees of Bishopdown Evangelical Church are the Data Controller, and the Church Secretary acts as our Data Protection Officer.

Why do we collect information?
We collect your personal data to help us:

- maintain our list of church members and regular attenders.
- provide pastoral support for members and others connected with our church.
- provide services to the community including, but not limited to, Parent & Toddler Group, Children's clubs, Tuesday Lunch.
- safeguard children, young people and adults at risk.
- recruit, support and manage staff and volunteers.
- maintain our accounts and records.
- respond effectively to enquirers and handle any complaints.

We use your information we hold to contact you and send you communications regarding our activities; to provide pastoral care and ensure the safety of your children while they are in our care. We are committed to complying with the law regarding data sharing and we do not share your information with others, except as described in this notice. We send information about our events and activities by e-mail, SMS, telephone and by post.

Storing your data
We hold data for varying lengths of time depending on the type of information and reason for keeping it. The data in question will always be kept in a manner which complies with the Data Protection legislation.

Who do we share you information with?
The information you give will only be shared with the leaders of the groups to which you are attached in the church eg: Noah's Ark, Lions Club, Kings Club, Lighthouse and Tuesday Lunch leaders who may need to contact you regarding the running of the group. This information will be kept for one year after our last contact with you (with the exception of the children's groups where we will hold it for up to three years in order to inform you of the other children's clubs or events we hold), or until you ask to be removed from the list. All leaders of the respective groups are aware of Data Protection legislation and will comply with it. We will not share your information with any other third parties.

Requesting access to your personal data
Under Data Protection legislation you have the right to ask to see the information we hold about you. You also have the right to ask for information you believe to be incorrect to be rectified. To make a request to see your personal information contact admin@bishopdownevangelicalchurch.org.uk. You also have the right to ask us to remove your details from our records at any stage by contacting us at admin@bishopdownevangelicalchurch.org.uk.

If you are concerned about the way your information is being handled please speak to our Data Protection Officer. If you are still unhappy you have the right to complain to the Information Commissioners Office.

Contact: Data Protection Officer via admin@bishopdownevangelicalchurch.org.uk