Eastwood Baptist Church
Data Protection Policy

Contents

Section A – What this policy is for

1. Policy statement

1.1 Eastwood 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 but not limited to Youth & Children's Ministries, Advice courses, Prayer Ministries and Women's Fellowship;
d) safeguard children, young people and adults at risk;
e) recruit, support and manage staff and volunteers;
f) undertake research;
g) maintain our accounts and records;
h) promote our goods and services;
i) respond effectively to enquirers and handle any complaints.

1.2 This policy has been approved by the church's Membership

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
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 a minister, employee, officer, trustee 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 Trustee 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 a trustee: 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 Data Protection Policy.

3.3 As a data subject of Eastwood Baptist Church: we will handle your personal information in line with this policy.

3.4 As an appointed data processor/contractor: Companies who are appointed by us as a data processor are required to comply with this policy under the contract with us. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the company or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (Eastwood Baptist Church) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

3.5 Our Data Protection Trustee is responsible for advising Eastwood Baptist Church 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 dataprotection@eastwoodbaptist.org.uk

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

3.7 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 Trustee.

Section B – Our data protection responsibilities

4. What personal information do we process?

4.1 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, DBS checks and those concerned with the data subject's pastoral care.

4.2 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, addresses, telephone numbers, email addresses, dates of birth, employment details and visual images of people.

4.3 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.

4.4 We will not hold information relating to criminal proceedings or offences or allegations of offences unless they are directly related to a safeguarding issue.

4.5 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.

5. Making sure processing is fair and lawful

5.1 Processing of personal data will be 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 personal data can be legally used

5.2 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 Eastwood Baptist Church 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 'special categories' of data can be legally used

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

a) the processing is necessary for carrying out our obligations under employment and social security and social protection law;
b) the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;
c) the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
d) the processing is necessary for pursuing legal claims.
e) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

5.4 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.

What individuals must be told before we use their data

5.5 If personal data is collected directly from the individual, we will inform them about the identity and contact details of the Data Protection Trustee, the reasons for processing, and the legal basis, explaining our legitimate interests and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement;

This information is commonly referred to as a 'Eastwood Baptist Church Privacy Statement' and can be found in Appendix two. Page 14>15
This will be publicly displayed at Eastwood Baptist Church so that is available to anyone. It is important that this information is available at the time when the personal data is collected.

6. When we need consent to process data

6.1 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.

6.2 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.

7. Processing for specified purposes

7.1 We will only process personal data for the specific purposes explained in our privacy notices (as described above in section 5.5) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described in section 5, unless there are lawful reasons for not doing so.

8. Data will be adequate, relevant and not excessive

8.1 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

9. Accurate data

9.1 As far as it is possible we will make sure that personal data held is accurate and, where appropriate, kept up to date.

10. Keeping data and destroying it

10.1 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.

10.2 Information about how long we will keep records for can be found in our Data Retention Schedule that is in Appendix 3 page 16>19

11. Security of personal data

11.1 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.

11.2 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:

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

11.3 Measures may include:

a) technical systems security;
b) measures to restrict or minimise access to data;
c) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
d) ensuring that personal information is transmitted securely in a way that cannot be intercepted by unintended recipients;
e) physical security of information and of our premises;
f) organisational measures, including policies, procedures, training and audits;

12. Keeping records of our data processing

12.1 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). This can be seen in our review of data found in appendix 3 page 16>19

Section C – Working with people we process data about (data subjects)

13. Data subjects' rights

13.1 We will process personal data in line with data subjects' rights, including their 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
g) withdraw consent

13.2 If a colleague receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Trustee immediately.

13.3 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.

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

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

14. Direct marketing

14.1 We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations 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)

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.

14.2 Any direct marketing material that we send will identify Eastwood Baptist Church 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

15. Sharing information with other organisations

15.1 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 persons are allowed to share personal data.

15.2 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.

16. Use of Electronic Communication

16.0 Email Protocols for staff and volunteers sending out EBC emails
All staff and administration & finance volunteers should have a church email address.

16.1 Only church email addresses should ever be used to process (i.e.: receive, share, send) any documents, data, or any other information relating to church business.

16.2 Every person sending emails in their capacity as an employee or volunteer of the church must read this Data Protection Policy and understood their role and responsibilities.

16.3 Emails received that contain any personal data must be processed in line with the church's Data Retention Schedule.

16.4 When sending personal data to a third party, reasonable attempts should be made to verify that the identity of the third party is valid and that nobody else has access to their email address.

16.5 Emails should only be used to share personal data where this is in accordance with the processes set out in the Data Protection Policy.

16.6 When sending an email to multiple recipients, care should be taken not to inadvertently share email addresses amongst recipients by adding multiple addresses to the 'cc' box. The primary recipient should be added to the 'To' box, with all other recipients added to the 'bcc' box.

17. Data processors

17.1 Before 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.

17.2 We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract

18. ICO Registration

18.1 The Trustees of Eastwood Baptist Church believe that registration with the ICO is not necessary as we are a not-for-profit organisation that qualifies for an exemption. Eastwood Baptist Church qualifies because:

a) it only processes information necessary to establish or maintain membership or support;
b) it only processes information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
c) it only shares the information with people and organisations necessary to carry out the organisation's activities; and
d) it only keeps the information while the individual is a member or supporter or as long as necessary for member or supporter administration.

Section E – Managing change & risks

19. Data protection impact assessments

19.1 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 and using new technology.
DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'.

20. Dealing with data protection breaches

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

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

20.3 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.

20.4 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.

This Statement and Policy will be reviewed annually;

Initial Policy 2018

Last reviewed and revised June 2021

Appendix 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.

In Eastwood Baptist Church this role would be fulfilled by a Trustee and overseen by the Church Members' Meeting.

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 Statement	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: 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.

Appendix 2:

Eastwood Baptist Church's Privacy Statement

Under Data Protection legislation the Members of Eastwood Baptist Church are the Data Controller and the Data Protection Trustee acts as our Data Protection Officer.

For Communication and Pastoral Care:

We are collecting this information to enable the church to keep in touch with you and provide pastoral support as appropriate. Data Protection legislation allows us to process this information as we regard it as being in the church's legitimate interest.

Your name and contact details will be entered into our church database which is held on computers which are password protected and accessed only by the Minister, Church Secretary and those with good reason to access it.

Your contact details will be removed from the database once you are no longer a part of the church – unless you ask to remain as one of our "church friends". We would like to include your name and contact details in our Church Directory which will be distributed by email to all Church Members and in hard copy as appropriate.

A copy will also be kept in the church office and the Manse Office. We will not give copies of the Church Directory to anyone not named in the Church Directory. You can ask for your details to be removed at any time and they will not appear in the next directory. To enable us to provide adequate pastoral support to you and your family, one of the Ministers may record information which may be regarded as sensitive. This information will be stored in password protected technology. This information will NOT be disclosed to anyone else without your consent.

You have the right to ask to see any information we hold about you (including the pastoral support information) by submitting a 'Subject Access Request' to the Data Protection Trustee. You also have the right to ask for information which you believe to be incorrect to be rectified. 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.

For Children, Youth and Families' Work:

We collect information to enable the church to run its children, youth and families' work safely and ensure we can contact you (or other nominated adult) to update you with information or in case of an emergency.

Data Protection legislation allows us to process this information as we regard it as being in the church's legitimate interest. If you are unable to supply the information requested, then we will be unable to accept your child in our ministries.

The information you supply will be held in paper form in a folder which will be kept in a securely locked cupboard in the church office. Only staff and appointed volunteers will have access to this information. Contact telephone numbers may be stored by

the Minister and / or the children & families' work leaders on password / fingerprint secured technology.

Contact and health forms will be renewed each year (normally in September) and the old forms will be destroyed.
We will not pass on this information to anyone else. If you are concerned about the way your information is being handled, please speak to our Data Protection Trustee. If you are still unhappy you have the right to complain to the Information Commissioners Office.

Appendix 3: Review and Retention of Data at Eastwood Baptist Church

The following table describes data that the Church holds, why and for how long All documentation should be reviewed annually.

DOCUMENT	RETENTION PERIOD	REASON/ STATUTORY PROVISIONS	ACTION AFTER RETENTION PERIOD
Meetings			
Members' Meeting Minutes	10 years from the date of the meeting	Good Practice	Archive
Trustees/ Leadership/Deacons Meetings Minutes	10 years from the date of the meeting	Good Practice	Archive
Minutes of other internal group meetings	5 years from the date of the meeting	Good Practice	Secure disposal
Membership			
Church membership list	Permanent but reviewed annually and updated	Good Practice	Archived if church closes
Contact details of members and regular attenders	6 months after the individual has ceased to be a member of/or has stopped attending unless requested to be removed earlier by individual concerned	Good Practice	Secure disposal
Church Directory	3 years after publication	Good Practice	Secure disposal
Finance			
All financial records invoices bills and bank statements etc.	6 years from the end of the financial year the records relate to	HMRC Guidance and Charities Act	Secure disposal
Gift Aid declarations	6 years after the last payment was made	HMRC Guidance	Secure disposal
Legacy information	6 years after the deceased's estate has been wound up	In line with other financial information	Secure disposal
Annual Accounts and Reports	10 years	Good practice	Archive

DOCUMENT	**RETENTION PERIOD**	**REASON/ STATUTORY PROVISION**	**ACTION AFTER RETENTION PERIOD**
Payroll records and HMRC and pension correspondence	6 years from the end of the financial year the records relate to	HMRC Guidance and Charities Act	Secure disposal
Health and Safety			
Accident Book	3 years after date of entry or end of any investigation if later	RIDDOR The reporting of diseases and dangerous occurrences regulations 2013	Secure disposal
Records documenting external inspections	3 years after date of inspection	Good practice	Secure disposal
Insurance			
Public liabilities policies and certificates	Permanently	Historical claims	Secure storage with electronic back up.
Employer's liability policies	Permanently	Employer's liability [compulsory insurance] Regulations 1988 suggest 40 years	Secure storage with electronic back up.
Other insurance policies and schedules	Until claims under policy are barred or 6 years after policy lapses	Commercial practice	Secure disposal
Claims correspondence	6 years after last action	Commercial practice	Secure disposal
Property			
Title Deeds	Held by BUGB		
Leases	12 years after lease and liabilities under the lease have been terminated	Limitation Act 1980	Secure disposal
Buildings certificates, plans and drawings	Permanently	Limitation Act 1980	

DOCUMENT	**RETENTION PERIOD**	**REASON/ STATUTORY PROVISIONS**	**ACTION AFTER RETENTION PERIOD**
Fire Inspection Records	6 years	Annual review	Secure disposal
Gas and Electricity certificates	6 years	Annual review	Secure disposal
Employment			
All information relating to recruitment, selection and development	6 years after the post-holder ceases to be an employee	Limitation Act 1980	Secure disposal
Information on any disciplinary or grievenace matters	6 years after the post-holder ceases to be an employee	Limitation Act 1980	Secure disposal
Information on individual's health and sickness record	6 years after the post-holder ceases to be an employee	Limitation Act 1980	Secure disposal
Information on any safeguarding concerns or matters in which the employee was involved	75 years after the post-holder ceases to be an employee	Requirements of IICSA [independent inquiry into child sexual abuse	
Redundancy records	6 years from date of redundancy	Limitation Act 1980	Secure disposal
Parental leave records	18 years from the child's date of birth	To enable future employers to check entitlement	Secure disposal
Payroll records and related HMRC correspondence	6 years from the end of the financial year the records relate to	Charities Act and HMRC Guidance	Secure disposal
Pension records	According to the schedules set by Pensions provider		Secure disposal
Application forms and interview notes for unsuccessful candidates	1 year after interviews have been completed	Limitation Act 1980	Secure disposal
Complaints records		Limitation Act 1980	Secure disposal

DOCUMENT	**RETENTION PERIOD**	**REASON/ STATUTORY PROVISIONS**	**ACTION AFTER RETENTION PERIOD**
Safeguarding			
Records of safeguarding incidents, allegations or concerns	75 years after last contact with individual concerned	Good practice	Secure disposal
Records relating to concerns/allegations about employees or staff [paid or voluntary]	75 years after employment ceases	Good practice	Secure disposal
Risk assessments /contracts with known or alleged offenders	75 years after last contact with individual concerned	Good practice	Secure disposal
Register of events for children under 18 years/ adults at risk	4 years after the event	Good practice	Secure disposal
Parent/ carer consent forms for children/ adults at risk	4 years after the form has been completed	Good practice	Secure disposal
Risk assessments for events for children under 18 years/ adults at risk	4 years after the form has been completed	Good practice	Secure disposal
Records of DBS checks	75 years after role ceases	Good practice	Secure disposal
Records of staff [paid or voluntary]disciplinary procedures relating to safeguarding allegations or offences	75 years after role ceases	Good practice	Secure disposal
General			
Correspondence	Unless this relates to any category of data listed elsewhere, correspondence should only be kept for as long as it is relevant. An annual review of what is retained is good housekeeping practice.		
Digital recordings	One week	Good practice	Erasure

Appendix 4:

Conducting Data Protection Impact Assessments

The DPIA is one of the specific processes mandated by the General Data Protection Regulation (GDPR). Organisations must carry out a DPIA where a planned or existing processing operation – "is likely to result in a high risk to the rights and freedoms of individuals".

DPIAs are particularly relevant when considering any data that belongs to someone under 16 or an adult who is at risk. The ICO have said that they have a large concern about any data breaches concerning these vulnerable groups.

DPIAs should also be considered when introducing a new data processing system or technology.

A DPIA helps organisations to find and fix problems at the early stages of any project, reducing the associated costs and damage to reputation that might otherwise accompany a data breach.

Six key stages of the DPIA

DPIAs are scalable in length and scope, depending on the privacy risks and impact of the processing operation.

The key stages of the DPIA are:

1. **Identify the need for the DPIA** – determine whether the inherent risks of the processing operation require you to undertake a DPIA.
2. **Describe the information flow** – be able to describe how the information within the processing operation is collected, stored, used and deleted.
3. **Identify privacy and related risks** – catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data you collect and/or process.
4. **Identify and evaluate privacy solutions** – for each identified risk to the personal data, make a 'risk decision', i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.
5. **Sign off and record the DPIA outcomes** – record the outcomes of the DPIA (steps 1-4) in a report that is signed off by whoever is responsible for those decisions. Where a high risk has been identified, the organisation must submit the DPIA to the regulatory authority for consultation.
6. **Integrate the DPIA outcomes into the project plan** – you will need to continually refer to the DPIA in order to ensure that it is being followed and that its responses to the risks have been implemented effectively

Contact information for your Household

Surname†			
Christian Name†		**Spouse's Christian Name†**	
Date of Birth		**Spouse's Date of Birth**	
Address†			
Telephone Number†			
Mobile Number†		**Spouse's Mobile†**	
Email Address†		**Spouse's Email Address†**	
Child One†		**Date of Birth**	
Child Two†		**Date of Birth**	
Child Three†		**Date of Birth**	
Child Four†		**Date of Birth**	
Child Five†		**Date of Birth**	

Consent: I have read the EBC Privacy Statement and give my consent for my data to be used in this way.	**Signed:** (Person filling out form)	
Spouse's Consent: I have read the EBC Privacy Statement and give my consent for my data to be used in this way.	**Signed:** (Spouse)	
Under 16 Consent: I have read the EBC Privacy Statement and confirm that I have the right to give consent for those listed on this form who are under 16 and I consent for that data to be used as prescribed.	**Signed:** (Person filling out form)	
Photo Consent: I understand that photos are taken from time to time at church and those pictures are used to positively promote life at EBC. I give my consent for pictures that contain my image and those named that are under 16 to be used for this.	**Signed:** (Person filling out form)	
Spouse's Photo Consent: I understand that photos are taken from time to time at church and those pictures are used to positively promote life at EBC. I give my consent for pictures that contain my image to be used for this.	**Signed:** (Spouse)	

If you are unable to sign the 'photo consent' please be aware that when photos are being taken, we will give a verbal warning and hope that you able to place yourself out of shot.

Persons 16 and over must complete their own form