Wymondley Baptist Church

Data Protection Procedure for **Wymondley Baptist Church**

Last updated	15 April 2019

Definitions

The Church	Means Wymondley Baptist Church.
GDPR	Means the General Data Protection Regulation.
Responsible Persons	Means the Deacons/Trustees of Wymondley Baptist Church.
Register of Systems	Means a register of all systems or contexts in which personal data is processed, accessed or shared by the the Church.

1. Introduction

The Church is committed to processing data in accordance with its responsibilities under the GDPR as detailed in its Data Protection Policy.

This document details the procedures to be followed to comply with the Church's Data Protection Policy.

This document is structured in the form of repeating the policy and then stating the procedure that will be followed as sub-items, numbered using lower case Roman Numerals. Where there is no specific procedure to apply to an item in the Data Protection Policy then the wording of the policy is included with no sub-items listed below.

2. General provisions

a. This policy applies to all personal data processed by the Church.
b. The Responsible Persons shall take responsibility for the Church's ongoing compliance with the policy. The Church does not need to appoint a Data Protection Officer as detailed in the Church's Data Protection Policy.
c. This procedure shall be reviewed at least every three years along with the policy that it responds to.
d. The Church is not required to register with the Information Commissioner's Office as an organisation that processes personal data as detailed in the Church's Data Protection Policy.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Church shall maintain a Register of Systems.
    i. To achieve this a spreadsheet will be maintained that lists the types of data that are

held.

b. The Register of Systems shall be reviewed at least annually.
    i. Following the AGM the Register of Systems will be reviewed by a member of the Church Deacons/Trustees.
c. Individuals have the right to access their personal data and any such requests made to the Church shall be dealt with in a timely manner.
    i. Requests will be accepted with a signed request in writing or via email to the Church email address welcome@wymondleybaptist.org.uk.
    ii. A response will be given to the requester within 1 month of the request being received.
    iii. If this timescale cannot be met an initial reply will be provided advising when a final response will be provided.
    iv. The final response should not be more than 2 months after the date when the original request was received.

4. Lawful purposes

a. All data processed by the Church must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Church shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
    i. Where possible written consent will be received either via email or via a signed hard copy.
    ii. If it is not possible to receive explicit consent, for example for users of the Church's website, warnings will be displayed to inform people that their personal data will be held if they proceed.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Church's systems.
    i. People can request to be removed from communications via a signed request in writing or via email to the Church email address welcome@wymondleybaptist.org.uk.
    i. On receipt of a request to be removed from communications the appropriate group leader/administrator will be informed.
    ii. Communication will be ceased within 1 month of receipt of a request to be removed from communications.

5. Data minimisation

a. The Church shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
b. Consideration will be given to the data being held to confirm that the conditions of the Church's membership policy are met, for example that members are 16 years old or above.
    i. A membership form will be produced that includes the date of birth of the individual.
c. Consideration will be given to only process the personal data required to uniquely identify Church members as individuals for the purpose of maintaining a record of their Church membership.
    i. In order to uniquely identify members, the membership form will include individual's

full name and address, in addition to their date of birth as detailed in item **b i.** above.

d. Consideration will be given to allow Church members or those associated or having regular contact with the Church to opt in to share personal data with one another, for example email addresses or phone numbers. This will not exempt Church members or those associated or having regular contact with the Church from providing the Church with the personal data required for the effective running of the Church.
    i. The membership form described previously will include the option for individuals to clearly indicate their consent for which data they consent to be shared with others.
    ii. An enquirers form will be produced to allow individuals who are not Church members to clearly indicate their consent for which data they agree to be shared with others.
    iii. Where consent has been received to share an individual's data this data will not be shared with organisations/individuals outside the Church, without prior written permission received in writing and signed or via email to the Church email address welcome@wymondleybaptist.org.uk. This may include the Church Deacons/Trustees or other Church officers, e.g. Treasurer, Secretary etc, where personal contact details may need to be shared with outside organisations/individuals in order to allow them to fulfil the duties of their office.
    iv. To limit the chance of sharing individual's data, when communicating via email to a group, email addresses will be hidden to other recipients by use of the blind copy (bcc) feature of the sending email application, where possible, or by sending the same email to each individual one at a time.

6. Accuracy

a. The Church shall take reasonable steps to ensure personal data is accurate.
    i. The information held by the Church will be collected directly from the individual. Where the individual is under 18 years of age, then the information will be collected from their parent or guardian.
    ii. If any inaccuracy is in the data held by the Church then it will be corrected within 1 month of the issue being identified and confirmed to be accurate by the individual whose data was corrected, where possible.
    iii. If it is not possible to confirm the accuracy of the data held by the Church, then it will be deleted/destroyed unless it must be held for legal reasons (see Archiving/removal section below).
    iv. When data is required to be held for legal reasons, and it is suspected to be inaccurate and cannot be confirmed by the individual whose data it is, then a note will be kept with the data to indicate the nature of the concern.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
    i. As part of the annual review of the Register of Data any potential updates to data will be identified and updated within 2 months of the AGM.
c. Church members or those associated or having regular contact with the Church will be able to request that the personal data processed by the Church is updated.
    i. People can request that personal data processed by the Church is updated via a signed request in writing or via email to the Church email address welcome@wymondleybaptist.org.uk.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Church shall put in place an archiving policy for each area in which personal data is processed and review this process every three (3) years.
   i. As part of the annual review of the Register of Data any potential archiving of data will be identified and archived within 2 months of the AGM.
   ii. The above procedure will be reviewed every three (3) years as part of the review of the Data Protection policy.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.
   i. The data retention periods will apply as detailed in Appendix 1.
   ii. If the above data retention periods are not applicable, then Church members personal information shall be stored until either the individual resigns their membership, the member dies, or written notice is provided by the Responsible Persons that their membership is being cancelled.
   iii. If the above data retention periods are not applicable, then those associated or having regular contact with the Church will have their personal data removed after not attending any activity of the Church for a period of no more than two (2) years as long as the condition in the above data retention periods are not applicable.
   iv. Church members and those associated or having regular contact with the Church will have their personal data retained as required by the law to maintain records for the purposes of Safeguarding or any other statutory requirements. This period may be longer than the periods detailed above.
   v. The Church website and email servers will be backed up electronically as detailed in the contracts and agreements held with the platform providers and in-line with their data protection policies.

8. Security

a. The Church shall ensure that personal data is stored securely using physical security, such as lockable cupboards, or cabinets etc, when required. Where data is held electronically modern software that is kept-up-to-date will be used, including the use of passwords or other security measures.
   i. Where data is held electronically then the data will be held on a computer that has a user password or other security measure (for example finger print recognition etc) and the file will be password protected.
   ii. Where data is held electronically then the computer where the data is held will have an operating system that has on-going security update support from the software manufacturer.
   iii. Computers that hold personal data should have security updates installed as recommended by the software manufacturer.
   iv. Computers that hold personal data should check for, and install if required, security updates at a minimum once a year.
   v. The Church website and email servers will be secured as detailed in the contracts and agreements held with the platform providers and in-line with their data protection policies.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
   i. The Responsible Persons shall ensure that the personal data shared to other personnel

is required for their role and that appropriate permission has been received before sharing it.

ii. Personnel that are required to receive personal data will either receive a copy of the Church's Data Protection Policy and this Data Protection Procedure or be given access to read these documents electronically in order to ensure that they are familiar with their requirements.

iii. The Register of Systems will record who has been given access to personal data and in what form.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.
   i. Hard copies of personal data will be shredded.
   ii. Electronic copies of personal data will be deleted from all the computers and storage devices recorded in the Register of Systems, including all back-ups and recycle folders.

d. Appropriate back-up and disaster recovery solutions shall be in place.
   i. The Responsible Persons will make a duplicate copy of hard copies of personal data which will be held in a separate physical location to the original.
   ii. The Responsible Persons will make a duplicate copy of electronic versions of personal data on a separate storage device to the original, preferably the separate storage will be at a separate physical location to the original.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Church shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).

END OF PROCEDURE

Appendix 1 – Retention periods

Section	Documents	Retention period	Reason	Action after Retention Period
Employment/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)	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)	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)	Destroy
	Redundancy records	6 years from date of redundancy	Limitation Act 1980	Destroy
	Information on any safeguarding concern or matter in which the employee was involved in any way	75 years after employment/role ceases (see Safeguarding Retention Schedule under Safeguarding below)	Requirements of the Independent Inquiry into Child Sexual Abuse (IICSA)	Not applicable
	Parental leave records	18 years from the date of the birth of a child	To enable future employers to check entitlement	Destroy
	Payroll records including correspondence with HMRC	6 years from the end of the financial year the records relate to.	Charities Act and HMRC Rules	Destroy
	Pensions Records	According to the schedules set by the Pension provider		Destroy

	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.	Destroy
	Complaints records	1 year where complaint referred elsewhere otherwise 6 years from last action	Limitation Act 1980	Destroy

(1) Six years is generally the time limit within which proceedings founded on contract may be brought

Section	Documents	Retention period	Reason	Action after Retention Period
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	Destroy
	Gift Aid declarations	6 years after the last payment was made	HMRC Rules	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	Destroy
	Church Annual Accounts and Reports	10 years [(2)]	Good practice	Archive (e.g. County Archive Office)
	Payroll records including correspondence with HMRC	See Employment/HR above	See Employment/HR above	See Employment/HR above

(2) These should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the church before sent to archives.

Section	Documents	Retention period	Reason	Action after Retention Period
Health and 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	Destroy
	Records documenting external inspections	3 years after date of inspection	Good practice	Destroy

General	Correspondence (including emails)	Unless this relates to any other category of data listed here (e.g. finance, employment, safeguarding etc) correspondence should be kept for as long as is relevant. It is recommended that officers/staff and volunteers to have an annual 'purge' of all correspondence and destroy any which is no longer relevant.

Section	Documents	Retention period	Reason	Action after Retention Period
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	Destroy

	Claims correspondence	6 years after last action	Commercial practice	Destroy

Section	Documents	Retention period	Reason	Action after Retention Period
Meetings	Church Meeting Minutes	10 years from the date of the meeting (3)	Good practice	Archive (e.g. County Archive Office)
	Trustee Meeting Minutes	10 years from the date of the meeting (3)	Good practice	Archive (e.g. County Archive Office)
	Minutes of internal groups	5 years from the date of the meeting	Good practice	Destroy unless of particular value in which case send to Archive

(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.

Section	Documents	Retention period	Reason	Action after Retention Period
Membership	Church Membership List (Names)	Permanent but reviewed and updated regularly	Good practice	Archive if church closes
	Contact details of Church Members	6 months after individual has ceased to be a member of the Church. [4]	Good practice	Destroy
	Contact details of regular attenders (including guest speakers)	2 years after individual has stopped attending the Church. [4]	Good practice	Destroy
	Church Contact list or Directory	1 year after publication	Good practice	Destroy if it has been superseded or information is out of date

(4) Unless individual asks for their details to be removed immediately

Section	Documents	Retention period	Reason	Action after Retention Period
Property	Title Deeds for property (where church holds their own)	Permanently or until property is disposed of	Limitation Act 1980	Keep copy for 6 years after property has been disposed of
	Leases	12 years after lease and liabilities under the lease have terminated	Limitation Act 1980	Destroy
	Final plans, designs and drawings of the building, planning consents, building certifications, collateral warranties, records of major refurbishments and redevelopments.	Permanently or until six years after property is disposed of	Limitation Act 1980	Destroy 6 years after property is disposed of

Safeguarding	See separate Safeguarding Retention Schedule at www.baptist.org.uk/gdprsafeguarding