Weymouth Baptist Church
Data Protection Policy

Context and overview

Key details

- Policy prepared by: **Ted Winter**
- Approved by the Trustees on**: 15th February 2018**
- Policy became operational on: **20th February 2018**
- Next review date: **January 2019**

Introduction

Weymouth Baptist Church (WBC) needs to gather and use certain information about individuals.

These can include members, suppliers, business contacts, employees and other people the church has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the church's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures WBC:

- Complies with data protection law and follow good practice
- Protects the rights of members and other identifiable individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulation 2016 (GDPR) describes how organisations - including WBC - must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The Trustees of WBC
- All departments of WBC
- All staff and members of WBC
- All contractors, suppliers and other people working on behalf of WBC

It applies to all data that the church holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Identifiable photographic images and videos
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect WBC from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with WBC has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Charity Trustees** (Minister and Deacons) are ultimately responsible for ensuring that WBC meets its legal obligations. They are the **Data Controller**.

- The **Privacy Officer**, **Gary Spracklen**, is responsible for:

    - Keeping the Trustees updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from members and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data WBC holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the church's sensitive data.

- The **IT Manager**, **Ted Winter**, is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the church is considering using to store or process data. For instance, cloud computing services.

- The **Publicity Deacon**, **Ted Winter**, is responsible for:

    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other members to ensure marketing initiatives abide by data protection principles.

Definition of Personal Data

Personal data means information relating to a living being who can be identified from that data (or from that data plus other information in our possession).

Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal) or a statement of intent about them.

Personal data in electronic format also includes images of living individuals in digital photos and video, if the image is clear enough for particular individuals to be identified

It also includes “online identifiers” such as computer IP addresses and website cookies.

General guidelines for those accessing data

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, members can request it from the Data Controller.
- WBC will provide training to all those needing help to understand their responsibilities when handling data.
- Church members should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the church or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Members should request help from the Privacy Officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Members should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically** on a:

- Desktop/laptop/tablet computer e.g. within a file/folder or email
- Portable hard drive. CD, DVD, or USB memory stick
- Mobile phone e.g. text message, file or folder, email or voicemail
- Landline phone e.g. voicemail or fax machine

it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between members.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the church's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to WBC unless the church can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, members should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically.** The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Members **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy

The law requires WBC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort WBC should put into ensuring its accuracy.

It is the responsibility of all members who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Members should not create any unnecessary additional data sets.
- Members should **take every opportunity to ensure data is updated**. For instance, by confirming a contact's details when they call.
- WBC will make it **easy for data subjects to update the information** it holds about them. For instance, via the church's website or an appropriate form.
- Data should be **updated as inaccuracies are discovered**. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by WBC are entitled to:

- Ask **what information** the church holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the church is meeting its **data protection obligations**.

If an individual contacts the church requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller c/o office@weychurch.co.uk The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, WBC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Baptist Union's legal advisers where necessary.

Providing information

WBC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the church has a privacy statement, setting out how data relating to individuals is used by the church.

This is available on request to the church office. A version of this statement is also available on the church's website.