

Upper Stratton Baptist Church

'A heart for God and God's heart for others'



T: 01793 831535

E: admin@usbc.org.uk

www.usbc.org.uk

USBC Data Protection: Procedures and Guidelines

December 2018

Produced by the GDPR Working Group

Approved by: USBC Trustees

UPPER STRATTON BAPTIST CHURCH. GREEN ROAD, SWINDON, WILTSHIRE. SN2 7JA

MINISTER: REVEREND SIMON GOVIER

Upper Stratton Baptist Church is a Registered Charity No: 1133910 (Registered in England and Wales)

Table of contents:

Contents

Definitions:.....3

Overview:3

Individual consent:3

Email communications:3

Other communications:4

Breaches:4

Protecting data:4

Definitions:

GDPR Working Group: A group established by the Trustees to manage data protection on behalf of the church. The Trustees remain the legally responsible persons. Currently this group comprises three members: Minister, Head of Ministry for Finance, and Communications Officer but may change from time to time if requested by the Trustees. The group can be contacted through the church office or by emailing dataprotection@usbc.org.uk.

USBC Data Privacy Policy: A published policy document available through the church website at www.usbc.org.uk/dataprotection.

Breach: Any loss or unauthorised access, use or disclosure of personal information by the church or individuals acting on its behalf.

Administrator: A person employed by USBC, normally managing the church office workload.

Personal data: Any personal information held or processed by the church. See the Data Privacy Policy for details.

Approved systems: USBC may store and process personal data using various software and systems, in compliance with UK law.

Overview:

The guiding principle for USBC data protection should be to demonstrate the utmost respect for the privacy of all individuals. This approach will naturally affect our compliance with UK law.

Personal information should only be shared, whether verbally, in writing or by any other means with the express consent of the individual concerned. If consent has not been given then great care should be taken to ensure any information shared does not enable the individual to be identified, even if they are not named. For example, asking the church to 'pray for my friend who is ill' would be acceptable whereas 'pray for my next door neighbour who is ill' would require the neighbour's consent.

Individual consent:

The church maintains lists to safely manage bulk communications. Every individual can express and change their consent for various kinds of communications at any time at usbc.org.uk/dataprotection or by contacting the church office.

The 'members' email list is restricted to current Members of USBC. The Administrator will check this list regularly to ensure all subscribers are current members and move any that are not to the appropriate list (maintaining the same preferences).

Individuals involved in teams, home groups or other groups can give consent to the relevant group leader regarding communications about that group's activity.

An individual can give consent verbally or in writing for information about their health, personal circumstances or other information to be shared, specifying the methods they are consenting to. They may, for example, say they are happy for the information to be shared only within a group to which they belong, through the newsletter, in the Magazine, through the Prayer Chain or at a church service. It is important that their wishes are carefully respected by everyone.

It is especially important that we continue to develop the culture of respect for privacy amongst everyone attending services and groups.

Email communications:

Emails to more than 10 recipients will normally be sent through the church mailing list system. This system does not display details of other recipients and takes account of expressed consent.

Emails to smaller groups of recipients (such as teams) and to home group members may be sent through a standard email client. The sender should normally use BCC to prevent disclosure of other recipient's details. Small groups should also consider using social media groups (e.g. WhatsApp or Facebook closed groups) over which the group leader has control.

Other communications:

It is important that we respect expressed preferences when communicating. Our main communication system (currently Mailchimp) stores this consent and must always be referred to before data is used.

Breaches:

Anyone becoming aware of, or suspecting, a data breach should inform the church office immediately by telephone or email to dataprotection@usbc.org.uk.

Any alleged or suspected breach will be reported immediately to the GDPR Working Group who will begin an investigation within 24 hours. This Group will manage any required action including informing the Trustees if a breach is found to have occurred. All reports will be documented. The Trustees will be responsible for ensuring compliance with UK law, including reporting to authorities if required.

Protecting data:

All personal data held by the church must be treated with respect and protected from loss or unauthorised access.

Any device (whether personal or church property) with access to this data must be password protected and locked or shut down when unattended.

Loss of any device with access to data (whether personal or church property) must be reported to the GDPR Working Group immediately as action may be required to ensure data is protected from unauthorised access.

Data may only be stored on systems provided or authorised by the church. In particular, data should not be transferred by memory sticks or email unless suitably protected or encrypted. The GDPR Working Group can advise if required.

Training will be provided as necessary for use of approved systems. In particular, care and expertise must be exercised when using communications systems such as email and mailing list software.

Data stored in church systems should not be shared with anyone unless express permission has been given. This will be clear from the Mailchimp data. For example, details appearing in the Members Directory can be shared with other members (but not with non-members unless consent is obtained).

All personal data stored on paper must be locked in a secure cabinet. Information provided to members on paper which discloses their personal data (such as postal address) must be posted or handed out personally, not left in public areas for collection.

Where a member is acting on behalf of the church, such as organising an activity, the need for people to be able to contact them may outweigh the need for their express consent to publish their contact details (processing as a 'legitimate interest') though it is preferable to gain their consent if possible. The GDPR Working Group can advise if required.