Stoneygate Baptist Church
Data Protection Policy

Policy statement

Stoneygate Baptist Church (hereafter referred to as SBC) is committed to protecting all information that we collect and process about people, and to respecting their rights around how that information is handled. We value the information entrusted to us and we respect that trust, by complying with all relevant laws and adopting good practice, recognising the hurt that can be caused when that is not done. This policy explains our responsibilities and how we will meet them.

We process 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; safeguard children, young people and adults at risk; recruit, support and manage staff and volunteers; maintain our accounts and records; promote what we do; respond effectively to enquirers; and handle any complaints.

This policy has been approved by the church's trustees, who are responsible for ensuring that we comply with all our legal obligations. Anyone who processes personal data on behalf of the church must understand and adhere to this policy. To this end, we will provide training as necessary, to raise awareness of their obligations and our responsibilities, as well as to outline the law. We may also issue procedures, guidance or instructions from time to time.

SBC is registered with the Information Commissioner's Office, and Mark Burleigh is the named Data Controller for SBC. Any questions about this policy or any concerns that the policy has not been followed should be referred to him at treasurer@stoneygatebaptist.org.uk.

Collecting data

Data may be received straight from the person it is about, for example where they provide contact information in order to join our mailing lists. We may also receive information about data subjects from other sources, for example previous employers in the case of staff. 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 at which the data is collected. We will not collect more data than is needed to achieve the purposes named in this policy. We will not collect any personal data "just in case" we want to process it later. The accuracy of personal data will be checked at the point of collection and at appropriate points later on, in order to ensure that personal data held is accurate and kept up to date.

Processing data

Data may be processed in electronic or paper form, and both forms are covered by data protection law. The personal data we process includes information such as names and contact details, and visual images. In some cases, we hold types of information that are called 'special categories' of data in the GDPR. These may include details of pastoral and health issues, where this is important for caring for a person's physical or mental wellbeing. We will not hold information relating to criminal proceedings or offences or allegations unless there is an overarching safeguarding requirement, and this processing will only ever be carried out on advice from the BUGB Ministries Team or our Regional Association Safeguarding contact person. Bank details may be collected, but this information is not stored by the church, being held only within our online bank accounts. Alongside this Data Protection Policy, the church will maintain a Data Audit, so that it is clear what information is held and where.

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: the processing is necessary for a contract with the data subject; the processing is necessary for us to comply with a legal obligation; the processing is necessary to protect someone's life (this is called "vital interests"); the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law; the processing is necessary for legitimate interests pursued by SBC or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject. If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

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: the processing is necessary

for carrying out our obligations under employment and social security and social protection law; 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; 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; the processing is necessary for pursuing legal claims. If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

Where none of the other legal conditions apply to the processing, and we are required to obtain 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 can be withdrawn at any time, at which point the processing will stop. If anybody wishes to see the data the church holds about them, or remove their data from church records, they may submit a request to the Data Controller at treasurer@stoneygatebaptist.org.uk, and the data will be presented or deleted as requested. We will not keep personal data longer than is necessary for the purposes that it was collected for.

Storing data securely

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, and from accidental loss, destruction or damage. We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing. These will include ensuring all devices and online storage accounts used for processing data are password protected, with passwords only held by those with legitimate authority to access the information, and keeping all paper documents in locked containers.

Personal data cannot be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a “cloud” based service where the servers are located outside the EU. We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

Responsibilities of church members

The relational nature of churches means that members may hold information about others in the community, including contact details and sensitive information shared in prayer requests. The use of data by church members for personal reasons is outside of the remit of this data protection policy, but our duty of care to one another requires that we all treat the information shared with us respectfully.

Direct marketing and sharing data with third parties

Any direct marketing material that we send will identify SBC 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. 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, 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. 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.

Dealing with data protection breaches

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 trustee responsible for data protection. We will keep records of data breaches, even if we do not report them to the ICO. 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.

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.