Grace Baptist Church, Stockport

Privacy Policy

This policy has been drawn up to ensure *Grace Baptist Church, Stockport* meets the legal requirements of the General Data Protection Regulation (GDPR) which takes effect in British law on 25th May, 2018. An additional website privacy policy is available on our website detailing the specific requirements for users of the website.

Data Controller
The Data Controller is the Leadership team / church officers of *Grace Baptist Church, Stockport.*

Purposes for which Grace Baptist Church collects Personal Data
We process personal data to help us:

a) maintain our record of church members, past and present;

b) maintain records of official church meetings and charity trustee meetings;

c) provide a church address list of members and others associated with the church;

d) provide pastoral support for members and others connected with our church. This includes personal data recorded on prayer sheets for the purpose of prayer and support;

e) safeguard children, young people and adults at risk;

f) recruit, support and manage staff and volunteers;

g) maintain our accounts and records and

h) respond effectively to enquirers and handle any complaints;

Legal grounds for use of said data

1) Legitimate interests:

- The need to maintain our record of church members, past and present;
- The need to maintain records of official church meetings and charity trustee meetings;
- The need to provide pastoral support for members and others connected with our church;
- The need to safeguard children, young people and adults at risk;
- The need to recruit, support and manage staff and volunteers;
- The need to maintain our accounts and records and
- The need to respond effectively to enquirers and handle any complaints;

2) The data subject's explicit consent (or consent of parents / guardians for children under the age of 16, which they can withdraw at any time;

- If in the future the church provides a church address list of members and others associated with the church to those people;
- To maintain a list of young people attending church activities with contact details, consent for collection for church activities and required medical information
- Information given to share with members and others associated with the church for the purpose of mutual support and prayer.

3) Statutory requirements or contracts:

- Requirements of charity law
- Requirements of employment law

Length of time data will be retained, and the criteria used to determine it

- Official historical records such as the church membership book and records of members meetings will be stored permanently in a paper form. An electronic version of these records may also be kept securely permanently
- Employment and financial records will be kept according to official guidance about retention periods for specific records. If in doubt, records will be kept for 6 years, to cover the time limit for bringing any civil legal action.
- Records relating to children/young adults will be retained at least until the child/young adult reaches the age of 21 to comply with the Limitation Act 1980.
- If a church address list is maintained it will be updated on a regular basis to ensure data is up to date.
- Personal confidential information required for pastoral care (including prayer lists) will also be kept as required. Such data will frequently require retention on a long-term basis in order to provide ongoing pastoral care and demonstrate what care has been provided for individuals.

Rights of Data Subjects

- The right to withdraw consent at a later time. When this happens, the church will erase the individual's details except where data is required to be kept – for instance, for the purposes of pastoral care, for maintaining accurate records of church meetings, for demonstrating that individuals had a valid DBS check whilst engaged in church activities, etc. Frequently, data about current and past members will require retention to

demonstrate the procedures followed by the church in providing pastoral care or exercising church discipline.

- The right to be informed (i.e. that their data is being held, and for what purpose).
- The right of access to one's personal information (via a **Subject Access Request**). If a Subject Access Request is received the church will disclose to the individual what information is held on them by the church within 30 days. Confidential private data regarding a data subject, e.g. personal notes from meetings and communications between church officers, will not be disclosed since it is necessary for the pastoral care of individuals that such private information and communication remain private. However, any such data will be stored in accordance with the GDPR regulations.
- The right to rectification (i.e. correction of inaccurate data). This only applies to demonstrably inaccurate data and cannot be used to, e.g. change minutes of members meetings previously approved by a church meeting.
- The right to restrict processing. Note this clause cannot be used to prevent sharing of necessary information about an individual with the leadership of another church to who a former member or attendee is transferring membership or attendance. This might include e.g. details or disciplinary procedures or safeguarding concerns.
- The right to data portability (i.e. allows individuals to obtain and reuse their personal data for their own purposes across different services). Given the nature of the data held by the church it is not expected that this clause will be relevant.
- The right to object.
- The right to complain to the ICO

Data protection breaches

A *data breach* is any personal data seen by anyone not entitled to do so. A breach can also be considered to have occurred where data is misplaced or lost.

- In the situation where it is suspected that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to the Data Controller.
- We will keep records of personal 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.

Appendix

The GDPR regulations require that all personal data:

1) Shall be processed *lawfully, fairly, and in a transparent manner in relation to individuals (**lawfully*: the conditions for processing data have been met; *fairly*: the connection between the use for which the data was collected and the use to which it is put; *transparent:* the data subject is fully aware of how their data is being or will be used);

2) Shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

3) Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) Shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

5) Shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and

6) Shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

Furthermore:

7) The Data Controller shall be responsible for, and be able to demonstrate, compliance with these principles.

This last is the *accountability* principle, which requires Data Controllers to demonstrate *how* they comply with the principles – for example by documenting the decisions taken during the process of acquiring and storing data. *Grace Baptist Church* has met this requirement by a data audit in which the way data is handled and stored has been recorded.

Data Protection Officer

It has been determined that *Grace Baptist Church* does not currently require the appointment of a Data Protection Officer. This is on the basis that we **do not** meet the following requirements that need a Data Protection Officer:

- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

Information Commissioners Office (ICO) Registration

Under the 2018 Regulations, organisations that determine the purpose for which personal data is processed (controllers) must pay the ICO a data protection fee unless they are exempt. Grace Baptist Church, Stockport meets the exemption requirements on the following basis:

Generally speaking, you have to pay a fee if you are processing personal data as a controller. But there are some exemptions. You don't need to pay a fee if you are processing personal data **only** for one (or more) of the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Not-for-profit purposes
- Personal, family or household affairs
- Maintaining a public register
- Judicial functions
- Processing personal information without an automated system such as a computer

Grace Baptist Church meets this exemption requirement since we only process personal data under the three highlighted purposes:

Staff administration

This is processing for the purposes of appointments or removals, pay, discipline, superannuation, work management or other personnel matters concerning your staff.
 The individuals you hold information about will be restricted to any person whose personal information has to be processed for staff administration.

The term 'staff' includes all past, existing or prospective members of staff who are employees, office holders, temporary and casual workers, and also agents and volunteers. The personal information held about them includes all personnel and work management matters – for example their qualifications, work experience, pay and performance.

Accounts and records

This is processing for the purposes of keeping accounts relating to any business or other activity you carry out; deciding whether to accept anyone as a customer or supplier; keeping records of purchases, sales or other transactions to ensure the relevant payments, deliveries or services take place; or making financial or management forecasts to help you carry out your business or activity.
 The individuals you hold information about are restricted to anyone whose personal information needs to be processed for your accounts and records – for example past, existing or present customers or suppliers.

 The information you hold is restricted to personal information that is necessary for your accounts and records – for example, name, address and credit card details. However, the exemption specifically excludes information processed by or obtained from credit reference agencies.

Controllers who are providing accounting services for their customers are not exempt.

Not for profit purposes
A specific exemption applies to bodies or associations that are not established or conducted for profit. However, the exemption applies only if:

 you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it

 you only hold information about individuals whose data you need to process for this exempt purpose

 the personal data you process is restricted to personal information that is necessary for this exempt purpose

If yes to all – a data protection fee is not due

Glossary

Data means information relating to a *data subject* (i.e. a living person) who can be directly or indirectly identified from that data; whether the information is kept in paper records or on electronic devices such as a computer or smart phone. Data falls into two categories – **Sensitive Personal Data** and **Personal Data**:

· **Sensitive Personal Data** is any data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data (e.g. fingerprints), physical or mental health, sex life and/or sexual orientation. NB By this definition any data held by Grace Baptist Church should be considered Sensitive Personal Data since it implicitly or explicitly reflects religious beliefs.
· **Personal Data** is any other information relating to an identified or identifiable living person, such as their postal address.

Data *Protection* is a requirement placed on *Data Controllers* who process (see below) information about data subjects. Churches, in this context, are *Data Controllers*.

Process means to obtain, record, or hold data, or carry out any operation on the data.

Controller – a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor – a person, public authority, agency or other body which processes personal data on behalf of the controller.

Data protection officer – Under the GDPR, some organisations need to appoint a data protection officer who is responsible for informing them of and advising them about their data protection obligations and monitoring their compliance with them.

Data subject – the identified or identifiable living individual to whom personal data relates.