Glasgow Grace Church
Data Protection policy

Glasgow Grace Church is committed to following the principles of the UK Data Protection Act and to keeping the principles outlined in it. In particular, GCP seeks to ensure that the personal data it holds is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with an individual's rights to access, change the way it is processed, amend, alter or delete the data in line with the data subject's request
7. Kept securely
8. Subject to compliance with the principles of the General Data Protection Regulations (GDPR)

The GDPR applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that GCP holds in whatever form. The details of how these aims are achieved is worked out in the paragraphs below.

1) Registration

Glasgow Grace Church considers that it is not exempt from registration under the General Data Protection Regulations, and aims to be compliant with it in full.

2) Glasgow Grace Church Legitimate Interests

Glasgow Grace Church has a legitimate interest in collecting, processing and storing data for the purpose of developing a membership. The organisation presents its public benefit report in its annual accounts, and this public benefit is achieved through the development of a membership.

For example, when collecting information from guests at our times of meeting, we will generally use that data to contact the giver of said data in order to assist them with any queries that they have about the organisation's business or to support them in line with our charitable objectives. Our charitable objectives are aligned with the development of a membership and so we consider there to be a direct and legitimate connection between collecting personal data and the achievement of our charitable objectives.

For reasons of clarity, our charitable objectives are summarised as follows:

a) To advance the Christian faith in accordance with our statement of beliefs in Glasgow and beyond
b) To relieve sickness and financial hardship and to promote and preserve good health by the provision of funds, goods or services of any kind, including through the provision of counselling and support in Glasgow or beyond.
c) To further Christian education including but not by way of limitation to children of pre-school age in Glasgow or beyond.
d) To provide or assist in the provision of facilities in the interests of social welfare for recreation or other leisure-time occupation of individuals who have need of such facilities by reason of their youth, age, infirmity or disability, financial hardship or

social circumstances with the object of improving their conditions of life in Glasgow or beyond.

Personal data is collected, processed and stored with these objectives in mind, as a legitimate interest.

3) Data Management

Glasgow Grace Church uses password protected documents when storing any data and on computers with password protection and encryption.

4) Data subjects

'Personal data' means information about a living individual who can be identified from that information and other information which is in, or likely to be in, Glasgow Grace Church's possession.

With reference to point 2 above, Glasgow Grace Church primarily holds personal data on:

a) Staff, including former members of staff and potential new staff, with their consent
b) Visitors including those who have identified that they wish to be considered as members of Glasgow Grace Church, with their consent
c) It will store the data of future members of Glasgow Grace Church, with their consent
d) Where applicable, and with consent, contact details for parents/guardians and carers of children who attend programmed events and clubs at Glasgow Grace Church.
e) Others who have signed up for events, and groups at Glasgow Grace Church, with their consent.
f) Anyone who donates to Glasgow Grace Church and has signed a gift aid declaration
g) Anyone requiring a DBS certificate for work undertaken as a Glasgow Grace Church ministry

This list is not exhaustive – for example, Glasgow Grace Church may also hold data on referees of those holding paid or voluntary roles within the organisation.

Glasgow Grace Church also holds data on different supporting organisations, churches and trusts. Some of this data is not personal data – for example, the minister of a church is a matter of public record - and some data is effectively in the public domain but this does not necessarily reduce the responsibility to keep the requirements of the GDPR.

5) Good practice

a) Ensuring data is fairly and lawfully processed

Processing data has a wide meaning in the context of data protection and refers to any action involving personal information, including obtaining, adding, storing, viewing, copying, amending, extracting, deleting, disclosing or destroying information. Glasgow Grace Church will ensure that the data it holds is processed fairly. The main test for this will be the subject's permission and expectation, i.e. will Glasgow Grace Church staff and supporters feel this is a proper use of the information that is held?

In accordance with the GDPR, Glasgow Grace Church will always endeavour to be explicit about this by explaining what use the information supplied will be put to. More information about this can be found on our Privacy Statement, which is published on our website. For the most part, when collecting personal data, we will endeavour to communicate that:

- *We will use this information to keep you informed of* Glasgow Grace Church *activities*
- *The information on this form/connect card/registration material will only be used to consider your application* (Application form for church membership/employment/voluntary position/CRB)
- *Your email and/or postal address will be used to send you information about church life, or to help us to establish or maintain church membership and will not be passed on to anyone outside* Glasgow Grace Church*, except for the purpose of the above.*
- *Where data is used outside of the organisation, it will only be used for the purposes of the above, or within the wider context of church membership as expressed by the Advance partnership of churches to which we belong.*
- *Where this is the case, we will only ensure that your data is processed in countries that provide an adequate level of protection for your data or where the recipient provides appropriate safeguards, such as model contract causes, binding corporate rules, or mechanisms like the EU-US Privacy Shield framework.*

b) Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive

In order to be able to monitor and control what data is held and to meet the requirements of the GDPR, Glasgow Grace Church encourages the holding of personal data within defined IT systems and databases. Currently these are:

- Password protected documents for use by church leaders or trustees.
- In a locked filing cabinet, at the home of our Treasurer, for use by the Treasurer for the purpose of processing payments between the church and its members, and, for the processing of gift aid

Before designing sources for data capture, such as paper forms, response slips or web pages, the designer should review with staff each item captured to assess if it is relevant and how this information will be stored.

Personal data kept on a laptop then this data **must** be stored in a password protected document.

Personal contact data will not be passed to other organisations without the person's explicit permission or instruction.

Unless otherwise requested, Glasgow Grace Church intends to hold personal data for ex-members, and children who have participated in Gateway meetings or events, and records of any financial transactions, indefinitely for the purpose of safeguarding (especially for the purpose of retrospective investigation), and ensuring financial probity.

c) Ensuring data is accurate and up to date

Keeping data accurate and up to date is a difficult and ongoing task. Glasgow Grace Church will make every effort to do this such as:

- Updating the records when advised of changes in direct debit instructions.
- Updating members personal details when advised of changes.

Officers and members of staff in Glasgow Grace Church are encouraged to regularly review the personal data they hold for accuracy and develop procedures in this area to ensure compliance.

d) Ensure data is not kept for longer than is necessary

Glasgow Grace Church will continue to develop policies of securely destroying personal data when it is no longer needed.

- Applications for church membership when church membership ceases
- CRB disclosures as soon as a record is made of the disclosure number. In most cases this is immediate. We will however, keep an ongoing record of CRB numbers for safeguarding purposes.
- Personal information of guests (adult) within 12 months of consecutive non attendance at a Glasgow Grace Church Service or event (reviewed during annual risk assessment)
- Personal information of children (registration and attendance registers) after 6 years from last point of contact
- Gift aid envelopes after 6 years of cessation of an individual giving to the church

'Securely destroying' usually means the shredding of paper copies of data and the deletion of computer files, emails and database entries. When a computer is disposed of, computer hard drives **must** be cleaned with a "zero fill" secure deletion process or be physically destroyed before being removed from the building.

Officers within Glasgow Grace Church are encouraged to monitor the accumulation of personal data held and develop procedures in this area to ensure compliance.

e) Ensure data is kept securely

i) Network security

All personal data stored on a computer must be protected by a robust username and password for access. Passwords should be sufficiently complex and regularly changed. Staff **must not** share network usernames and passwords. Passwords for any computer system should not be written down on paper.

ii) Backups

Data is backed up for all staff via external hard drive

iii) Security of data in transit

When personal data needs to be transferred to other parties, care must be taken to ensure that the data cannot be accidentally disclosed to unauthorised recipients. Secure methods of data transfer need to considered in all cases - preferences should be given to methods that ensure the data is encrypted such as secure ftp or SSL connections.

If encrypted transfer is not possible, personal data must at least be password protected.

Email is not a secure way of transferring personal data, as potentially an email can be read at any intermediate server. If personal data is sent by email it is recommended that the files be password protected before being emailed.

USB data sticks represent a very high risk area for the security of data, because they are so easily lost. Personal data **must not** be stored on personal data sticks belonging to officers or members of staff.

Laptops also represent a high risk area. If personal data needs to be kept on a laptop then the laptop must be password protected for access by the owner only. Whilst laptops remain the property of the church, they have been assigned to staff

and some volunteers for the purpose of the charitable objectives of the church. In this regard, responsibility for the security of the laptop and the data therein remains the responsibility of the assigned user wherever reasonably possible.

iv) Home and remote working

When working from home or other locations outside the office, staff **must** maintain appropriate levels of security, including physical security of printed material and data.

Special care should be taken in the transport of personal information to and from home.

v) Guarding against disclosure

All officers should ensure that personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

vi) Third Parties

Some third parties may on occasion obtain information pertaining to a Glasgow Grace Church Member for the purpose of auditing or payroll. These third parties are made aware of our Data Protection Policy as part of our condition of usage of said function, i.e. accounting and auditing.

vii) Breach of data

Immediately following any breach or loss of data, this should be reported to the Church Leadership and a nominated trustee. They shall determine whether said breach should be reported to the police. The decision for this should be based on whether the breach of data has resulted due to theft/fraud, or if there are any significant safeguarding issues to be considered as a result of the breach.

Any major breach of data will be reported to the Information Commissioners Office within 72 hours of the breach

As part of the annual risk assessment an assessment of the impact of data breach will be done and reported to the trustees.

6) Training

a) Staff

As part of the induction process, each member of staff will receive basic awareness training in the principles of GDPR and a copy of this document, as well as a copy of our privacy statement. This session will cover the principles outlined above and will also address particular issues that they may have within their job description.

b) Volunteers

Volunteers who work with personal data will be given a copy of this document, a copy of our privacy statement, and the ongoing opportunity to raise any questions or concerns related to the safe collection and processing of data.

7) Right to access information

Staff, supporters, and other data subjects have the right to access any personal data that is being kept about them by Glasgow Grace Church either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the church office. Glasgow Grace Church aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In

such cases, the Trustees will explain the reason for the delay in writing to the data subject making the request.

Similarly, Glasgow Grace Church recognises that all data subjects can at any time exercise their 'right to be forgotten'

Under certain circumstances, Glasgow Grace Church may disclose personal information to the police and other law-enforcement bodies. Glasgow Grace Church will do this only if it considers the request reasonable and proportionate.

8) Compliance

Compliance with the GDPR and with this policy is the responsibility of all members of staff and any volunteers who have been entrusted with personal data. Any deliberate or reckless breach of this policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with trustees in the first instance.

June 2018

Appendix A – Advice to Volunteers

Glasgow Grace Church is committed to following the principles of the General Data Protection Regulations and to keeping the principles outlined in it. In particular, we seek to ensure that the personal data we hold is:

1) Fairly and lawfully processed
2) Processed for limited purposes
3) Adequate, relevant and not excessive
4) Accurate and up to date
5) Not kept for longer than is necessary
6) Processed in line with an individual's rights for access, amendment or deletion of their data.
7) Alterable in the way that it is used by us upon request of the data subject (the person who's data is in question)
8) Kept securely
9) Not transferred to other countries without adequate protection

The GDPR applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that we hold in whatever form. We work out the details of how we achieve these aims in our Data Protection policy.

As a volunteer working for, or serving Glasgow Grace Church, you are required to follow the same procedures as staff in the handling and processing of data. If you are in doubt, please ask to see the entire data protection policy and ask for further advice.

The main issues that may arise will be:

1) **Ensure data is kept securely**
   a) Please make sure that the data you have been given is kept securely, whether in paper or electronic form. If travelling by public transport, keep them within your other luggage as you travel so that there is no risk of items being left on a train, or similar.
   b) USB data sticks are notoriously easy to lose. Please do not transfer personal data to these data sticks, unless they are encrypted.
   c) When working from home, you **must** maintain appropriate levels of security, including physical security of printed material and data.

2) **Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive**

   Please ensure that the data you have been given is only used for the purpose intended and is not given to or shared with anyone else. The data must be destroyed/deleted once it is no longer needed for that purpose.