
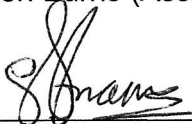



Data Protection Policy

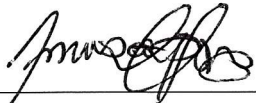
Agreed and accepted by the Elders and Trustees

Signed  Dated 17/7/22
Name Glen Burns (Assistant Minister and Elder)

Signed  Dated 17/7/22
Name Simon Abrams (Elder and Trustee)

Signed  Dated 17/7/22
Name Robert Honeysett (Elder and Trustee)

Signed  Dated 30/7/2022.
Name Ravi Srinivasan (Elder and Trustee)

Signed  Dated 17/7/2022
Name Kobby Sarpong (Trustee)

The policy will be reviewed annually.

Table of Contents

Introduction	3
Compliance with Data Protection by Design	3
Compliance with 6 Principles of Processing Personal Data	3
Compliance with Guidelines Relating to Rights of Individuals	5
Compliance with Privacy and Electronic Communications Regulations (PECR).....	8
Use of Emails	10
Use of WhatsApp Groups.....	10
Appendix 1: Information Security Policy	11
Appendix 2: Personal Data Breaches.....	13
Appendix 3: Assessment of legitimate interests as a lawful basis.....	14
Appendix 4: Use of consent as a lawful basis	14
Appendix 5: Special Category and Criminal Offence Data	15

Introduction

Grace Church Brockley (GCB) takes seriously the need to protect the personal data of individuals who come into contact with our organisation. This policy sets out procedures to be followed to ensure compliance with legislative requirements. It covers both GCB and the Christians Against Poverty (CAP) Lewisham Debt Centre that is coordinated by GCB.

Key staff, leaders and administrative support individuals at GCB and the Debt Centre (DC) will be provided with training on data protection and must agree to comply with this Data Protection Policy.

Please note that processing of DC client data, including financial data, is covered by CAP's central data protection policy. This policy covers processing of DC staff and volunteer data.

Legislative requirements: GCB adheres to all relevant data protection laws, including the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

Personal data: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' Examples of personal data include address, telephone number, bank details.

Compliance with Data Protection by Design

Data protection is incorporated into GCB's data processing activities through compliance with this Data Protection Policy and our Information Security Policy.

- See Appendix 1 for GCB's Information Security Policy

In addition, GCB holds a log of all categories of personal data held by the church. The log is reviewed annually by the individual designated by the Trustees as responsible for ensuring compliance with the data protection legislation and approved by the Trustees.

Compliance with 6 Principles of Processing Personal Data

1. Data will be processed lawfully, fairly and in a transparent manner

GCB/DC will not process personal data unless there is a lawful basis for doing so. To ensure there is legal justification, a log of personal data processed by GCB/DC is maintained. The log lists data by category, and documents the lawful basis for processing. The lawful bases are set out in Article 6 of the GDPR and include consent, contract, legal obligation and legitimate interests.

- See Appendix 3 for information on assessing legitimate interests.
- See Appendix 4 for information on obtaining consent.

Special category data and criminal offence data are particularly sensitive types of personal data and have additional requirements.

- See Appendix 5 for information on how GCB processes these data.

To ensure transparency, GCB/DC will inform data subjects about the data being collected and processed by GCB/DC. Clear information on the subject's rights (see below) is available in a Privacy Notice available on GCB's website.

2. Data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

GCB's log of personal data records the purpose(s) for which data are collected. If the purpose(s) change a formal review of the legal requirements is carried out.

3. Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

An annual review of GCB's log of personal data is carried out to check that this principle continues to be met. Action is taken (e.g. destruction of irrelevant data) as appropriate.

4. Data will be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Data accuracy is considered during the annual review of GCB's log of data. Appropriate actions are taken to ensure continued accuracy. (e.g. providing data subjects with a copy of their data for checking).

5. Data will 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 are processed

An annual review of GCB's log of data is carried out to check that this principle continues to be met. Action is taken (e.g. destruction of irrelevant data) as appropriate.

6. Data will 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 organisational measures

Personal data is held in accordance with GCB's Data Security Policy. In the event of a personal data breach, one of the church elders or trustees must be informed *immediately*. They will follow the guidance on data breaches appended to this policy.

- See Appendix 1 for GCB's Information Security Policy
- See Appendix 2 for instructions to be followed in the event of a data breach.

Compliance with Guidelines Relating to Rights of Individuals

Prior to responding to a request from an individual relating to personal data, verify the person's identity. Individuals have rights over their own data and data relating to their children. For individuals known to GCB/DC this may be straightforward, e.g. recognition of name and email address. For individuals not personally known by GCB/DC, use two independent ways of contacting the individual if possible (e.g. email and mobile).

1. Right to be informed including privacy notices

Whenever personal data is collected by GCB/DC we will ensure that the data subject is informed of:

1. What information is being collected
2. Who is collecting the data (i.e. GCB)
3. Who it will be shared with
4. How long it will be held
5. The purpose of the processing of their data
6. The lawful basis on which their data is being processed
7. The rights they have in relation to the data held about them (e.g. access, rectification)
8. Their right to withdraw consent (if relevant)
9. Their right to lodge a complaint with the ICO

This information will be provided at the time of collection of the personal data.

2. Right of access

If an individual requests access to their personal data the following steps will be taken.

1. Identify all possible personal data held by GCB. This requires a review of GCB's personal data log by relevant people, including staff team members, a finance representative and leaders of groups that the requester was linked with (e.g. fellowship group or befriender's team).
2. Provide information and obtain confirmation of receipt.
3. Retain a record of the access request, data provided and confirmation of receipt. This information will be retained for as long as GCB/DC holds personal data relating to the data subject.

3. Right to rectification and data quality

If an individual requests rectification of their personal data the following steps will be taken.

1. Make corrections in line with the request.
2. Provide data subject with a copy of the updated information and obtain confirmation in writing that the updated information is correct.
3. Retain a record of the request for rectification and confirmation that the data have been rectified. This information will be retained for at least 2 months and for a maximum of 2 years.

Refer to section on ensuring accuracy of data for instructions relating to general data quality control.

4. Right to erasure including retention and disposal

If an individual requests erasure of their personal data the following steps will be taken.

1. Determine the reason for erasure.
2. In general, requests for erasure will be complied with even if the requester does not meet any of the statutory reasons to have their data erased. Data **MUST NOT** be erased if there is a valid legal reason to retain them. Reasons for retention for GCB are:
 - a. to exercise the right of freedom of expression and information;
 - b. archiving purposes in the public interest, scientific research historical research or statistical purposes; or
 - c. the exercise or defence of legal claims.

N.B. data relating to safeguarding, including attendance registers, records of recruitment decisions, or documented safeguarding concerns must not be erased. Data relating to financial information must not be erased within 6 years of the financial year-end in which the transaction took place.
3. Erase the data and send written confirmation of this to the data subject, or inform the subject in writing that the data will not be erased, giving reasons for non-erasure.
 - a. Paper records will be shredded.
 - b. Electronic records will be deleted and appropriate checks made that there is no audit trail remaining.
 - c. If data was passed to third parties the request for erasure will be forwarded and steps taken to ensure it is complied with.
4. Where erasure of data has been refused, retain a record of the request and reasons for non-erasure. This information will be retained for as long as GCB holds personal data relating to the data subject. Where erasure has been completed, an anonymised record of the request and actions taken will be retained.

Refer to section on general data retention for instructions relating to general data retention timelines.

5. Right to restrict processing

If an individual requests GCB to restrict the processing of their personal data the following steps will be taken.

1. Where possible, annotate the data subject's personal data to show it must not be further processed. Notify the staff team, admin support and others who have access to the data.
2. Notify the data subject that the restriction is in place.
3. Retain a record of the request and the reply. This information will be retained for as long as GCB holds personal data relating to the data subject.
4. Prior to destruction of the subject's data, notify them of the proposed destruction and preferably obtain their consent.

6. Right of data portability

In the unlikely event that an individual requests transfer of their personal electronic data, the following steps will be taken:

1. Check if the request is permitted in law. Data portability only applies if processing is based on the individual's consent or for the performance of a contract.
2. Liaise with IT support to prepare and supply the required data. It must be provided in a common, machine-readable format (e.g. CSV or XML).

7. Right to object

If an individual objects to the processing of their personal data the following steps will be taken.

1. Check if the request is permitted in law. Individuals have the right to object to processing for direct marketing. In some situations they can object to processing based on 'legitimate interests'. Reasons to refuse the request are: GCB can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.
2. For personal data that falls under the 'Right to object', notify the data subject that these data will be destroyed. Preferably obtain their consent to this. Erase the data (see above) and send written confirmation of this to the subject.
3. Notify the subject of any personal data that is processed by GCB and does not fall under the 'Right to object'. Retain a copy of this notification for as long as GCB holds personal data relating to the data subject.

8. Rights related to automated decision making including profiling

At GCB no decisions are made, relating to individuals, on the basis of automated processing of data. This section is therefore not applicable.

If an individual exerts any of rights 2 to 8 above:

- GCB has one month in which to comply. Extensions are sometimes allowable.
- GCB will nominate an individual from within the staff team or admin support to be responsible for carrying out the appropriate steps.
- Current advice will be obtained from the ICO website.
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>
- The request (and any clarifications) will be documented, e.g. in a log.
- GCB will not charge a fee.

Compliance with Privacy and Electronic Communications Regulations (PECR)

Electronic Marketing

The PECR rules restrict unsolicited (not requested) marketing by electronic means, including phone calls, emails, texts and internet messaging.

- 'Marketing' covers all advertising, promotional and marketing material, including promoting the aims or ideals of GCB or the DC or seeking funding.
- Opt-in consent is needed before sending unsolicited electronic marketing directly to an individual.
- Opt-in consent must be specific about the type(s) of electronic communication used (phone, email, etc).

There are some exceptions:

- The PECR rules do not apply to solicited (requested) marketing. If someone specifically asks for information about GCB/DC, the requested information (only) can be sent.
- The PECR rules do not apply to marketing that is not sent directly to specific individuals. For example, GCB/DC can market an event on a public Facebook page or send leaflets that are not individually addressed.
- The PECR rules apply to organisations and not to individuals. This means church members/DC volunteers can send 'marketing' information to friends. For example, they could forward the above Facebook post. Take care that the communication is sent in a private capacity and not on behalf of GCB/DC.
- The 'soft opt-in' consent allows organisations to market similar information to past commercial customers. For example, GCB can market an event to those who attended a previous similar event. But – there must have been the option to opt-out and this must be repeated when contacting them again.

Electronic communications from GCB/DC are classified as either marketing or operational. Operational relates to activities or topics that an individual is already involved in. Marketing relates to activities or topics they are not already involved in. Marketing communications must only be sent to individuals who have given their specific consent to receiving them. Individuals may opt-out at any time.

Cookies

Where non-essential cookies are used by GCB's website, users will be informed what the cookies are doing and why. User consent will be obtained to store cookies on their devices, unless exemptions apply (e.g. the cookie is essential to provide the service requested).

Church Members' Directory/Volunteer Contact List

Note: the Information Commissioner's Office guidance states that church membership contact lists are not covered by the PECR.

GCB policy requirements are that individuals must give their written consent for inclusion in GCB's online directory or the DC's volunteer contact list and may opt-out at any time.

Use of Third Party Providers

Where GCB uses a third-party data processor (e.g. database provider), GCB is liable for processor's compliance with the UK data protection legislation. Therefore, the processor must provide sufficient guarantees that legislative requirements will be met, for example through a written contract setting out responsibilities and liabilities, or by review of information provided by the company.

GCB may use a range of different third party providers to store our data and provide website, social media, media, IT and system administration services. These processors include:

- Website platforms, website design companies, databases and event management systems including ChurchBuilder (part of Concordant Systems Ltd), Tiger Finch Creatives Limited, WordPress and WooCommerce (Part of Automattic)
- Companies processing payments (e.g. ticket sales) including PayPal and Stripe.
- Social Media and communication platforms including* Gmail, WhatsApp, Facebook, Spotify, Twitter
- Professional advisers including lawyers, bankers, auditors, pension advisors and insurers based in the UK who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities based in the UK who require reporting of processing activities in certain circumstances.

See the following websites for GDPR/privacy information for third party providers:

- Concordant Systems: <https://www.churchbuilder.co.uk/z/faqs29>
- Tiger Finch: <https://www.tigerfinch.com/privacy-notice/>
- WordPress: <https://wordpress.org/about/privacy/>
- WooCommerce (Part of Automattic): <https://automattic.com/privacy/>
- PayPal: <https://www.paypal.com/uk/webapps/mpp/ua/privacy-full>
- Stripe: <https://stripe.com/gb/privacy>
- Gmail: <https://policies.google.com/privacy>
- WhatsApp: <https://www.whatsapp.com/legal/privacy-policy>
- Facebook: <https://www.facebook.com/business/gdpr>
- Spotify: <https://www.spotify.com/uk/legal/privacy-policy/>
- Twitter: <https://gdpr.twitter.com/en.html>

Use of Emails

Emails should be blind copied to multiple recipients unless the sender is sure that all recipients have given consent to share their email addresses with one another.

Wherever possible, personal data will not be included in emails. Instead, personal data should be passed on face-to-face or by telephone, or saved in a secure area of the GCB website and a link emailed. When necessary to send personal data by email, the amount of data sent will be kept to a minimum and anonymised where possible.

Risks associated with emailing include:

- Hacking of email accounts
- Email 'tails' being forwarded inappropriately and/or
- Emails being sent to an incorrect recipient.

Longer term risks include:

- Storage of personal data (within emails) for longer than agreed retention time.
- Difficulties of meeting our obligations in the event that an individual requests access to all their personal data, including any held within emails.

Use of WhatsApp Groups

Personal WhatsApp groups set up by members of GCB are not covered by data protection legislation.

Official WhatsApp groups set up by GCB to communicate church-related information will be run in accordance with the following guidelines.

- The group will be set up by a member of the GCB leadership.
- Consent: the group will contain only GCB members who have consented to sharing their data with others who will be in the WhatsApp group. Consent should be documented (e.g. consent previously documented in church website/database). Potential group members may be sent a link to join the group in order to confirm their consent to join.
- Only GCB leaders will have admin permissions to enable them to add new members to the group or to remove members.
- For larger WhatsApp groups, usually only GCB leaders will have admin permissions to post information. For smaller groups (e.g. Fellowship Groups), the group may be interactive.

Appendices

Appendix 1: Information Security Policy

GCB's staff team and individuals providing leadership, administrative and/or organisational support to the staff team must read and agree to follow GCB's Information Security Policy. This will therefore include:

- All staff members (GCB/DC);
- All members of Church Council;
- Those leading Fellowship Groups;
- Those leading DC teams (e.g. prayer support team)
- Those leading Crèche, Children's Church, Onyx & Christians In Action (CIA);
- Those involved in managing GCB's finances; and
- Members of the evangelism committees and those involved in organising ad-hoc events, such as Word Alive

GCB holds personal data of people associated in some way with the church or DC. GCB also holds financial data relating to the organisation. GCB does not have a physical church office or building and data is held in people's homes or is web-based. Note that DC client data is covered by CAP policies.

- **Low risk data** – The majority of personal data held by GCB/DC and relating to church members or DC volunteers are low risk. Examples include names, addresses, telephone numbers. The data is not particularly sensitive and does not relate to vulnerable groups.
- **Medium risk data** – Data relating to children is categorised as medium risk and has additional safeguards in place.
- **High risk data** – Data relating to safeguarding issues, including recruitment of leaders and befrienders, safeguarding concerns, allegations and actions relating to these are categorised as high risk. Financial data such as information on salaries, donations, bursaries are also classified as high risk.

Security Requirements for All Categories of Data

Paper and electronic information held in people's homes must be kept securely.

For paper data: keep out of sight (e.g. in a drawer) in an area of the home not used by visitors. Shred when no longer required.

For electronic data: store on computer(s) that have firewall, virus protection and password access. Update passwords regularly. Ensure data is removed from computers prior to disposal. Avoid storage on USB sticks unless password protected. Avoid emailing of data where possible, particularly if medium/high risk.

Google Cloud and Dropbox should not be used for storage of personal data. These platforms do not provide sufficient security and do not restrict movement of data outside the UK.

Security Requirements for Medium Risk Data

For paper data: keep in a locked drawer, cupboard or room. Exception: temporary storage of data for short-term use (e.g. registers printed for use in next few days).

For electronic data: the requirements for all categories of data will be followed.

Medium risk data will be shared on a need-to-know basis.

Security Requirements for High Risk Data

For paper data: keep in a locked drawer, cupboard or room.

For electronic information the requirements for all categories of data will be followed.

High risk data will be shared on a need-to-know basis in a very limited manner.

Risk Management

GCB's staff team and individuals providing leadership, administrative and/or organisational support to the staff team will continually assess risks to the data held by GCB/DC. Concerns will be raised with the Trustees without delay and appropriate action taken.

Appendix 2: Personal Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In the event of a suspected data breach, GCB will nominate a lead person who will coordinate the investigation and ensure appropriate action is taken. The following guidelines should be followed.

1. Determine whether the breach has occurred and the extent of the data breach.
2. Take appropriate steps to prevent further breaches:
 - Close existing access
 - Prevent similar illegal access
3. Mitigate any potential side effects and damage caused by the breach.
4. Determine whether GCB is required to notify the Information Commissioner's Office (ICO). A breach must be notified if it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Notification must be in a specific format (refer to ICO website) and must be within 72 hours.
5. Determine whether GCB (or the DC) is required to notify the data subjects concerned. Subjects will usually have to be notified if the breach is likely to result in a high risk to their rights and freedoms. Notification should take place without undue delay. Consider informing subjects even if not required by law, to show transparency of data processing by GCB/DC.
6. Determine whether other bodies need to be informed of the data breach, such as the Charity Commission or CAP.
7. Maintain a record of the breach and the actions taken. Avoid including personal data within the documentation.

Refer to the ICO website for guidance in the event of a data breach.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

Appendix 3: Assessment of legitimate interests as a lawful basis

Legitimate interest is likely to be appropriate if you use people's data in ways they would reasonably expect and that have minimal impact on privacy or there is good justification for processing. Use this 3-part test (called a legitimate interests assessment or LIA).

- **Purpose test:** are you pursuing a legitimate interest? These can be your own interests or the interests of third parties. They can include commercial interests or individual interests. Consider why you are processing the data, who benefits and how.
- **Necessity test:** is the processing necessary for that purpose? If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply
- **Balancing test:** do the individual's interests override the legitimate interest? You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. Areas you might consider: are the data particularly sensitive or private? Do they relate to children or vulnerable groups? What impact will the processing have on the individual? Are they likely to object? Can you include an opt-out?

Decide whether you think legitimate interests is an appropriate basis. If you are unsure, it may be safer to look for another lawful basis.

Keep a record of the LIA and decision taken.

Review the LIA if there is a change in the processing.

Appendix 4: Use of consent as a lawful basis

If you decide to obtain consent for processing the data you hold this will need to be given clearly using a separate form from other information you provide (e.g. not included with general terms and conditions). Consent must be given to each separate processing activity (e.g. if you wish to carry out 6 different actions, the data subject must consent to all of them).

Consent must meet the following requirements:

- Freely given
- Given for a specific purpose only
- Informed – i.e. it must be clear what the individual is giving their consent to
- Obtained using positive opt-in – i.e. not pre-ticked boxes or inferred from silence or inactivity.
- Properly documented
- Easily withdrawn – there must be simple ways for people to withdraw consent

You must name your organisation and any third parties who will be relying on the consent.

Appendix 5: Special Category and Criminal Offence Data

GCB processes special category data relating to religious affiliation and health.

These data are processed under the following UK GDPR Schedule 1 conditions:

- Religious affiliation data relating to employment: Article 9(2)(b) Employment, social security and social protection law
- Religious affiliation data other than employment-related data: Article 9(2)(d) Not for profit body
- Health data: Article 9(2)(a) Explicit consent

GCB processes criminal offence data obtained through job application forms, job interviews, DBS checks and self-declaration forms. Criminal offence data arising from disciplinary action or safeguarding allegations will also be processed by GCB. These data are processed under the following conditions set out in Schedule 1 of the DPA 2018:

- Criminal offence data relating to employment: Condition 1 - Employment, social security and social protection
- Criminal offence data relating to working with children or adults in need of care and support: Condition 18 - Safeguarding of children and individuals at risk

Criminal offence data is not processed under Condition 29, consent, for the following reasons. Consent is not possible for employee or volunteer data because provision of DBS check related data is a condition of working in this area. Consent is not possible for data relating to safeguarding allegations because processing is a legal requirement.

GCB's compliance measures and retention policies for special category and criminal offence data are set out in the following documents.

- Measures taken to ensure compliance with the data protection principles in Article 5 of the UK GDPR – refer to this data protection policy
- Information provided to data subjects – refer to GCB's Privacy Notice
- Information on lawful basis and retention periods – refer to GCB's log of personal data