Data Protection

This is the Data Protection Policy of Grace Church

Version: 2.0

Grace Church Policy Reference: No. 11

Policy adopted by Trustees: 11th May 2023

To be reviewed bi-annually or sooner in the light of new recommendations

Date to be reviewed: 11th May 2025

Introduction

This policy outlines the basis on which Grace Church processes personal data.

"Data Protection Legislation" means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

The Data Protection Legislation ("the Legislation") is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully, and that where necessary the privacy of individuals is respected.

Our statement of general policy is:

- To comply with both the law and good practice by keeping good quality information securely in the right hands.
- To respect individuals' rights, giving them as much choice as is possible and reasonable over what data is held and how it is used.
- To be open and honest with individuals whose data is held.
- To provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.
- To request active consent for data to be processed as per privacy information notice.
- To ensure 'Privacy by default and design' in all systems, with organisational and technical measures in place to demonstrate Data Protection is a key consideration.

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the operations Manager.

Sia Hima, Operations Manager, on behalf of the Board of Trustees

Reference to other Policies and Procedures

This Data Protection Policy should be read in conjunction with other relevant policies and procedures covering:

- Retention of Data and Records Guidelines
- Information Security Policy
- Privacy Notice
- Privacy Impact Assessment Form
- Data Breach Notification Procedure
- Data Subject Request Procedure

Data Protection principles

Grace Church is committed to working with personal information lawfully and correctly. To this end *Grace Church* adheres to the principles detailed in the *Data Protection Act 1998* and *General Data Protection Regulations (2018)*. These principles require that personal information shall:

- be processed fairly and lawfully
- be obtained for specified lawful purposes and used only for those purposes
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for any longer than required for those purposes
- be secure and in a system that permits the easy identification of the data subject
- protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction
- be used in a way which complies with the individual's rights (this includes the right to be forgotten, right of access, right to rectification, right to be informed, right to restrict processing and right to object).
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action. Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Grace Church will not contact individuals for marketing purposes unless specific consent has been given

Employees and others who process data on behalf of Grace Church should assume that whatever they do with personal data will be considered to constitute processing. Individuals should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll
- If neither of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

The processing of children's data (i.e. under the age of 16) requires explicit parental consent. This means that *Grace Church* will obtain and be able to verify parental consent.

Monitoring the use of personal data

Grace Church are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data.
- employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored.
- All employees must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy.
- Spot checks may be carried out.
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the Data Protection Compliance Manager. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

Grace Church will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing.

- Manual records relating to church members or staff will be kept secure in locked cabinets. Access to such records will be restricted. Computer files should be password protected.

- We will ensure that staff and members who handle personal data are adequately trained and monitored.
- We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.
- We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).
- Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop should be password protected.

Data Retention

Grace Church will keep personal information for no longer than is necessary. The data retention requirements vary according to type and may be governed by statutory regulations. All data and records will be stored in accordance with the security requirements of the Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle, everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the Data Compliance Manager in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

Sensitive data

Grace Church will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.