

# GRACE CHURCH HAMMERSMITH

## *DATA PROTECTION POLICY*

### Contents

Changelog	1
Contents	1
<b>Policy Document</b>	<b>4</b>
Introduction and context	4
Processing personal data	4
Compliance with the Legislation	5
Sensitive data	6
Monitoring the use of personal data	6
The rights of individuals	7
Changes to this policy	8
<b>Appendices</b>	<b>9</b>
APPENDIX 1 - Information security policy	9
Review of Appendix	10
APPENDIX 2 - Records Retention Policy	11
Storage of Data and Records Statement	11
Guidelines for Retention of Personal Data	11
Types of Data & Suggested Retention Period	12
Personnel files, including training records and notes of disciplinary and grievance hearings.	12
Application forms / interview notes	12
Information relating to children	12
Church member information	12
Church group member information	12
Income Tax and NI returns, including correspondence with tax office	12
Statutory Maternity Pay records and calculations	12
Statutory Sick Pay records and calculations	13

Wages and salary records	13
Accident books, and records and reports of accidents	13
Health records	13
Student records, including academic achievements, and conduct	13
Review of appendix	13
APPENDIX 3: Data Breach Policy	14
Introduction	14
Purpose	14
Scope	14
Types of breach	14
Reporting an incident	14
Containment and recovery	15
Investigation and risk assessment	15
Notification	15
Evaluation and response	16
Review of appendix	16
APPENDIX 4: Data Protection Complaints Process	17
Review of appendix	17

# Policy Document

## Introduction and context

“Data Protection Legislation” means the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the General Data Protection Regulation (GDPR), any laws in the UK enacting the GDPR or preserving its effect in whole or part following the departure of the UK from the European Union and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, together with, 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. During the course of the activities of Grace Church Hammersmith (“the Church”), the Church Elders, Staff, and Trustees (“we”) will collect, store and process personal data about our members, people who attend our services and activities, employees, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in the Church. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held<sup>1</sup> by Rob Ilderton (one of the named trustees)

Email: [admin@gracechurchhammersmith.org](mailto:admin@gracechurchhammersmith.org)

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 Data Protection Compliance Manager.

## Processing personal data

All personal data should be captured, stored, and 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 any information relating to an identified or identifiable living individual. It includes, for example, employee data and factual information about a person, such as a name, address, or date of birth. It also includes recorded opinions about an individual, their actions

---

<sup>1</sup> As of 29 October 2024

and behaviour. It does not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered.

Examples of personal data are employee details, including employment records, names and addresses (digital and physical) and other information relating to individuals, including digital details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images. It also includes Church-run WhatsApp groups and other digital communications.

Employees and others (including members, volunteers, and trustees) who process data on behalf of the Church (referred to in this policy as “Employees”) should assume that whatever they do with personal data will be considered to constitute processing.

Employees should only process data:

1. If they have consent to do so; **or**
2. If it is necessary to fulfil the mission of Grace Church Hammersmith in serving its members and regular attendees (its “legitimate Interests”), unless this is overridden by the interests, rights and freedoms of the data subject<sup>2</sup>; **or**
3. If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll.

If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

## Compliance with the Legislation

Employees who process data on our behalf (such as to organise a church rota, or issue information relating to a church event) have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly, lawfully and transparently;
- be obtained for specified, explicit and legitimate purposes and used only for those purposes (in other words, cannot be gathered generically for all future potential use);
- be adequate, relevant and limited to the minimum necessary for those purposes;
- be accurate and kept up to date (every reasonable endeavour should be used to ensure personal data that is not accurate are corrected or erased without delay);
- be processed in a manner that ensures its security<sup>3</sup>;

---

<sup>2</sup> If in doubt about legitimate interest, speak with the named data protection compliance officer

<sup>3</sup> See Information Security Policy, [Appendix 1](#)

- not be kept for any longer than required for those purposes<sup>4</sup>

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 (in a privacy notice) unless there is a legal exemption from doing so. We will keep records of any information shared with a third party including a record of any exemption which has been applied.

Employees should follow the Data Breach Procedure<sup>5</sup> if they think they have accidentally breached any provision of this Data Protection Policy.

### **Sensitive data**

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards are deployed. Sensitive data means data consisting of information relating to an individual's<sup>6</sup>:

- Racial or ethnic origin;
- Banking and financial information;
- Political opinions;
- Religious beliefs;
- Trade union membership;
- Physical or mental health, and genetic information;
- 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.

Sensitive data may be processed in the course of our legitimate activities, but may not be passed to any third party without the express consent of the data subject (or for other legally mandated purposes).

Sensitive data should be stored and processed with enhanced security commensurate with the level of sensitivity, with all due diligence taken to secure it both at rest and in transit.

---

<sup>4</sup> See Retention Policy, [Appendix 2](#)

<sup>5</sup> [Appendix 3](#)

<sup>6</sup> This is an exemplar list of covered areas - as a general guide, any area which could embarrass, inconvenience or pose problems for an individual and which wouldn't typically be available via open source datasets such as the electoral roll should be treated as sensitive

## Monitoring the use of personal data

We 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;
- Employees must follow the Breaches Procedure<sup>7</sup> should they become aware of any breach of this policy;
- Employees will keep clear records of our processing activities and of the decisions we make concerning personal data (including reasons for the decisions) to show how we comply with the Legislation;
- 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 officer and provided to the Trustees.
- At the discretion of the Officer, a more detailed audit of data processing may be commissioned
- Data breaches will be
  - recorded and
  - investigated to see what improvements can be made to prevent recurrences<sup>8</sup>;
- We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements or where full compliance with the UK legislation is not relevant. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Commented [1]: Need to explore whether this is an issue with any current service providers (Churchsuite, Instagram, etc. etc.)

## 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 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.

The individual rights listed above are, however, not absolute and must be proportionally balanced against broader obligations of our church, including the rights of other individuals. In

---

<sup>7</sup> [Appendix 3](#)

<sup>8</sup> A good example of incident postmortem culture is described [here](#) with a template for this sort of review [here](#)

particular, certain kinds of data, such as employee references and disciplinary procedures, whose untimely disclosure could prejudice proceedings, are exempted.

Any request for access to data under the Legislation should be made to the Church Administrator (admin@gracechurchhammersmith.org) 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.

### **Changes to this policy**

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.

Policy adopted on **24 June 2022**.  
(Date TRUSTEES meeting)

Reviewed on 11 September 2023

Reviewed on 29 October 2024 and approved by Trustees on XYZ

### **APPENDICES**

**APPENDIX 1 – Information Security Policy**

**APPENDIX 2 – Records Retention Policy**

**APPENDIX 3 – Data Breach Policy**

**APPENDIX 4 – Complaints process**

# Appendices

## APPENDIX 1 - Information security policy

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

'Church data' means any personal data processed by or on behalf of Grace Church Hammersmith.

Information security is the responsibility of every member of staff, trustee, office holder, church member and volunteer using Church data on but not limited to the Church information systems. This policy is the responsibility of the current named Data Protection Compliance Officer who will undertake supervision of the policy.

Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- All data will be stored in a secure location, and precautions will be taken to avoid data being accidentally disclosed.
  - Where this location is digital (such as dropbox or similar), all endeavours will be taken to ensure that the storage facility complies with GDPR and other legislation
- Manual records relating to church members or staff will be kept secure in **locked** cabinets. Access to such records will be restricted, and recorded by the Data Protection Compliance Officer in a **log**.
- Access to systems on which information is stored must be password protected with strong passwords<sup>9</sup>
  - These should be changed at once if there is a risk they have been compromised.
  - Passwords must not be disclosed to others.

Commented [2]: Do we have one of these?

Commented [3]: Should create one of these if we don't have them

<sup>9</sup> Current guidance for password strength should be followed. For example, see <https://www.cisa.gov/secure-our-world/use-strong-passwords>

- We will ensure that staff and members who handle personal data are adequately trained<sup>10</sup> and monitored to ensure data is being kept secure.
- We will ensure that only those who need access will have access to data.
- 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 above<sup>11</sup>), e.g. password protection for documents and encryption<sup>12</sup> of data stored and at rest.
- 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 (who will be treated as data processors - see below).
- We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
- Appropriate software security measures will be implemented and kept up to date.
- We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
- Where personal devices are used to store or process personal data, they must be subject to appropriate security.

Commented [4]: Should schedule some training

All breaches of this policy must be reported to Rob Ilderton, or in his/her absence the Church Administrator (admin@gracechurchhammersmith.org).

## Review of Appendix

This policy will be regularly reviewed and updated.

Policy adopted on **24 June 2022**

To be reviewed every 12 months

Reviewed 29 October 2024

<sup>10</sup> For example, <https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/>

<sup>11</sup> See [Sensitive Data](#)

<sup>12</sup> For example, see [Dropbox](#) provisions, [Google Drive](#) provisions and [Churchsuite](#) provisions

## APPENDIX 2 - Records Retention Policy

### Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection 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.
2. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.
3. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed.
4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. If in doubt, take advice from the Data Protection Compliance Officer
5. Any data file or record which contains personal data of any form can be considered as confidential in nature.
6. Data and records should not be kept for longer than is necessary.
  - a. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".
  - b. All staff, trustees, volunteers and members of the Church are required to have regard to the Guidelines for Retention of Personal Data attached hereto.
7. Any data that is to be destroyed must be appropriately disposed of (for example by shredding).
  - a. Any group which does not have access to a shredder should pass material to the current Data Protection Compliance Officer who will undertake secure shredding.
8. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Church Leadership team to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of.

Policy adopted on **24 June 2022**

(Date of Church Trustees/Leaders meeting)

Reviewed on 29 October 2024

### Guidelines for Retention of Personal Data

Special care will be given to the lifecycle of personal and sensitive personal data, which is wont to grow stale. Higher classification of data should be stored with higher diligence of security, and destroyed more securely.

If you have any queries regarding retaining or disposing of data please contact the Data Protection Compliance Officer.

## **Types of Data & Suggested Retention Period**

### **Personnel files, including training records and notes of disciplinary and grievance hearings.**

- 6 years from the end of employment

### **Application forms / interview notes**

- Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.

### **Information relating to children**

*NB. You may find it helpful to read the following article: <http://safeinchurch.org.uk/record-retention> (currently at <https://christiansafeguardingservices.phasic-ltd.co.uk/record-retention>)*

- Check for accuracy once a year
- Record that child was a member of the group – permanent
- Secure destruction of personal data other than name and fact of membership – three years after cease to be a member

### **Church member information**

- Check for accuracy once a year
- Record that adult was a member – permanent
- Secure destruction of personal data other than name and fact of membership – three years after cease to be a member

### **Church group member information**

- Check for accuracy once every two years
- Record that adult was a member of group – permanent
- Secure destruction of personal data other than name and fact of membership – three years after cease to be a member

### **Income Tax and NI returns, including correspondence with tax office**

- At least 6 years after the end of the financial year to which the records relate

### **Statutory Maternity Pay records and calculations**

- As Above (Statutory Maternity Pay (General) Regulations 1986)

**Statutory Sick Pay records and calculations**

- As Above (Statutory Sick Pay (General) Regulations 1982)

**Wages and salary records**

- 6 years from the tax year in which generated

**Accident books, and records and reports of accidents**

- (for Adults) 3 years after the date of the last entry
- (for children) three years after the child attains 18 years (RIDDOR 1985)

**Health records**

- 6 months from date of leaving employment (Management of Health and Safety at Work Regulations)
- Health records where reason for termination of employment is connected with health, including stress related illness
  - 3 years from date of leaving employment (Limitation period for personal injury claims)

**Student records, including academic achievements, and conduct**

- At least 6 years from the date the student leaves in case of litigation for negligence

**Review of appendix**

This appendix will be regularly reviewed and updated.

Policy adopted on **24 June 2022**

To be reviewed every 12 months

Reviewed 29 October 2024

## **APPENDIX 3: Data Breach Policy**

### **Introduction**

Grace Church Hammersmith (“we”) hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

### **Purpose**

This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the Church.

### **Scope**

The policy relates to all personal data held by Grace Church Hammersmith, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the Church. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach, minimising harm to and supporting those affected by any breach.

### **Types of breach**

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- Theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

### **Reporting an incident**

Any person using personal data on behalf of Grace Church Hammersmith is responsible for reporting data breach incidents immediately to the named Data Protection Compliance Officer (Rob Ilderton).

Rob Ilderton: Email: admin@gracechurchhammersmith.org

The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

#### **Containment and recovery**

The Data Protection Compliance Officer will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police (or other appropriate authorities, such as the Charity Commission or Information Commissioner's Office) should be informed.

Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

#### **Investigation and risk assessment**

An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The Data Protection Compliance Officer will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

This investigation will be written up and stored in an appropriate location, and shared with the trustees in due course.

#### **Notification**

The Data Protection Compliance Officer will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case-by-case basis. The Information Commissioner will be notified, if at all possible within 24 hours of the breach, if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on

when and how to notify the ICO is available on their website <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.

The Data Protection Compliance Officer will keep (or cause to be kept) a record of all actions taken in respect of the breach, commonly called an 'incident log'.

#### **Evaluation and response**

Once the incident is contained, the Data Protection Compliance Officer will carry out (or commission an appropriate trustee or third party to carry out) a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

#### **Review of appendix**

This appendix will be regularly reviewed and updated.

Policy adopted on **24 June 2022**

To be reviewed every 12 months

Reviewed 29 October 2024

## APPENDIX 4: Data Protection Complaints Process

Grace Church Hammersmith (“we”) take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the Data Protection Compliance Manager without delay.

Rob Ilderton, the current DPCM, can be contacted as follows: Email:  
admin@gracechurchhammersmith.org

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner’s Office at <https://ico.org.uk/concerns/>

Any complaint received by us must be referred to the Data Protection Compliance Officer who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.
2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.
4. At the conclusion of the investigation, the Data Protection Compliance Officer will reflect on the circumstances and recommend any improvements to systems or procedures.

Commented [5]: We should have a 'complaints log' or similar to store this

### Review of appendix

This appendix will be regularly reviewed and updated.

Policy adopted on **24 June 2022**

To be reviewed every 12 months

Reviewed 29 October 2024