Hamilton Road Baptist Church
Data Protection Policy (UK GDPR, 2025 Edition)

CONTENTS

---

1. Introduction

Hamilton Road Baptist Church ("the Church") gathers and uses certain information about individuals.
This includes members, employees, volunteers, suppliers, service users, residents, and other people we have a relationship with or may need to contact.

This policy describes how personal data must be collected, handled, stored and deleted to meet data protection standards and comply with applicable law.

1.1 Why This Policy Exists

This data protection policy ensures that we:

- Comply with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.
- Follow good data protection practice.
- Protect the rights of members, staff, and volunteers.
- Are open and transparent about how we process personal data.
- Protect ourselves from the risks of a data breach.

1.2 Data Protection Law

The UK GDPR and the Data Protection Act 2018 set out how personal data must be handled.

These laws require that personal data shall be:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and kept up to date.
5. Retained only as long as necessary.
6. Processed securely.
7. **Accountability:** The Church is responsible for, and must be able to demonstrate, compliance with these principles.

1.3 Policy Scope

This policy applies to all staff, post-holders, volunteers, contractors, suppliers, and other people processing personal data on behalf of the Church, whether stored digitally, on paper, or in any other format.

It applies to all data relating to identifiable individuals, including:

- Names, contact details, and family relationships.

- Sensitive data (e.g., health, religious belief, ethnicity, sexual orientation).
- Digital identifiers such as IP addresses or cookies (where applicable).

1.4 Data Protection Risks

This policy helps protect the Church from:

- Breaches of confidentiality.
- Failing to offer appropriate consent or choice.
- Reputational damage caused by data loss or hacking.

---

2. Responsibilities

All who handle personal data must follow this policy and UK GDPR principles.

- **Trustees:** have overall accountability for compliance.
- **Data Protection Lead (DPL):**
  - Monitors compliance and advises on responsibilities.
  - Oversees data protection training.
  - Handles Subject Access Requests.
  - Reviews contracts with data processors.
  - Maintains breach and retention logs.
  - May act as the Church's Data Protection Officer if required.

Failure to comply may result in disciplinary action.

---

3. General Staff, Leader & Volunteer Guidelines

- Access personal data only if required for your role.
- Do not share data informally or externally without authorisation.
- Use strong, unique passwords and **multi-factor authentication** where available.
- Lock screens when unattended; secure all paper records in locked cabinets.
- Dispose of data securely (e.g., shredding, encrypted deletion).
- Use encrypted email or secure file transfer for sensitive data.
- Contact the DPL if unsure about data handling.

---

4. Data Collection and Processing

Personal data will be processed only where a lawful basis applies, typically:

- Legitimate interests of the Church that do not override individual rights.
- Compliance with legal obligations (e.g., employment, safeguarding).
- Consent, where required and freely given.

Consent must be **informed, specific, and unambiguous**.

4.1 Processing in Line with Data Subject Rights

Individuals have the right to:

- Access their personal data.
- Rectify inaccuracies.
- Erase their data ("right to be forgotten").
- Restrict or object to processing.
- Data portability (receive a copy in machine-readable form).
- Object to automated decision-making and profiling.

4.2 Data Protection Impact Assessments (DPIAs)

Before introducing new technologies or systems that involve significant personal data (e.g. online registration), a DPIA must be completed and approved by the DPL and Trustees.

---

5. Data Storage

- Paper records must be locked away when not in use.
- Digital data must be stored only on approved, encrypted drives or cloud services.
- MFA and antivirus protection must be enabled.
- Data backups are made regularly and securely stored.
- Personal data must not be stored solely on personal devices.
- Apply a "clear desk" policy.

---

6. Data Retention and Secure Destruction

Data will be retained only as long as necessary for the purpose collected.

Secure destruction will be carried out using an **approved data destruction provider**. Digital data will be deleted or irreversibly wiped when no longer required.

6.1 Retention Periods (Summary)

Data Type	Retention Period	Notes
Financial Records	7 years	Legal requirement
Member & Attendance Records	1 year after departure	Delete unless consent to retain
Employee Records	3–6 years (statutory), up to 7 if needed	Review annually
Safeguarding / Criminal Records	10 years (to age 21 if minor)	Secure storage only
Minute Books	Indefinite	Restricted access
Emails & Correspondence	Review annually	Delete if no longer needed

---

7. Data Use

- Lock computers when unattended.
- Use secure methods for file sharing and data transfer.
- Do not use personal devices for storing church data.
- Anonymise or pseudonymise data where practical.
- Only Trustees may authorise data transfers outside the UK, and only to GDPR-compliant providers.

---

8. Data Accuracy

We will take reasonable steps to keep data accurate and up to date.

- Encourage individuals to update information regularly.
- Perform annual data audits.
- Correct inaccuracies promptly when discovered.

---

9. Subject Access Requests and Disclosures

All individuals may request access to their personal data.
Requests should be submitted to the DPL in writing or by email.

Responses will be provided **without undue delay and within one month** (extendable by two months for complex cases).

9.1 Disclosing Data for Other Reasons

We may disclose data without consent if required by law, to protect vital interests, or to cooperate with statutory authorities (e.g. safeguarding concerns).

9.2 Providing Information to Data Subjects

We will issue **Privacy Notices** explaining how personal data is used, retained, and protected.
These are available on the Church website and updated annually.

---

10. Security Breach Management

Any suspected or confirmed data breach must be reported immediately to the DPL.

The DPL will:

- Record all incidents in the Breach Register.
- Assess severity and notify the **Information Commissioner's Office (ICO)** within 72 hours if required.
- Notify affected individuals if there is a high risk to their rights or freedoms.
- Present quarterly summaries to the Trustees.

---

11. Review and Version Control

This policy will be reviewed **annually** by the Data Protection Lead and approved by the Trustees.

Version	Date Approved	Approved By	Next Review	Summary of Changes
4.0	Nov 2025	Trustees	Dec 2026	Updated for UK GDPR, modern security, and DPIAs

---

Glossary of Key Terms

(Updated for UK GDPR)

Personal Data: Any information that identifies a living individual.
Special Category Data: Data revealing religious beliefs, health, ethnicity, etc.
Data Subject: The individual to whom the data relates.
Data Controller: The Church, determining the purpose and means of processing.
Data Processor: A person or organisation processing data on behalf of the Church.
Pseudonymisation: Replacing identifiers with artificial values.
Encryption: Securing data using mathematical algorithms and secret keys.
DPIA: Assessment of risks when introducing new data processing activities.
ICO: Information Commissioner's Office — the UK supervisory authority for data protection.

Signed – Mo Cameron 05/11/25