



Data Protection Policy

The Lighthouse Church

Version Control Sheet

Title	Data Protection Policy
Purpose	To outline the requirements for Lighthouse Church to comply with the Data Protection Act 2018
Author	Dele Bamgboye
Approved by	Administration
Date	03/03/2025
Version	1
Status	DRAFT
Review Frequency	Annually
Next Review Date	07.07.2027

Amendment History/Change Record

Date	Version	Key Changes / Sections Amended	Amended By

Contents

1. Introduction
2. Policy Statement & Scope
3. Principles
4. Data Protection Officer
 - 4.1 Requirement & Role
 - 4.2 Contact details
 - 4.3 Training and Awareness
5. Security and Information We Hold
 - 5.1 Privacy Notice
6. Rights of Individuals
 - 6.1 Summary of Rights
 - 6.2 Requests for disclosure of Personal Information (Subject Access Requests)
7. Legal Basis for Processing Personal Data
 - 7.1 Lawful Processing
 - 7.2 Statutory obligations
 - 7.3 Consent
 - 7.4 Processing of Children's Data
 - 7.5 Retention
8. International Transfers
9. Breaches and / or Complaints
10. Record of Processing Activity (ROPA)
11. Data Minimisation

1. Introduction

At TLHC, we are committed to safeguarding the personal data of our members, visitors, and staff. As a faith-based community, we understand the importance of trust and confidentiality, and we are dedicated to handling your personal data with the utmost care and respect.

This Data Protection Policy outlines our commitment to protecting your privacy and ensuring compliance with relevant data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. As the Data Controller, TLHC is responsible for processing personal data in a secure and transparent manner.

We collect and process personal data to support our mission, provide pastoral care, manage church activities, and engage with our community. This policy explains what personal data we collect, how we use and protect it, and your rights regarding your personal data.

Our goal is to create a safe and welcoming environment where you can freely participate in our church activities, knowing that your personal data is protected.

2. Policy Statement and Scope

TLHC is committed to safeguarding the personal data of our members, visitors, and staff. As a faith-based community, we recognize the importance of trust and confidentiality and are dedicated to handling personal data in accordance with the General Data Protection Regulation (GDPR).

In fulfilling our mission and serving our community, we collect, process, share, and dispose of personal information securely and correctly. This includes sharing information internally and with trusted partners to improve our services, prevent and detect fraud, and comply with our legal obligations.

We process all personal information in accordance with GDPR provisions. The lawful and correct treatment of personal information is essential to our ministry's successful operations and maintaining the confidence of the individuals to whom the data relates, both internally and externally.

TLHC requires all staff, volunteers, and third parties operating on our behalf to comply with this policy and cooperate with all measures and procedures in place to ensure legal compliance.

We fully endorse and adhere to the principles of data protection, ensuring that personal data is processed lawfully, fairly, and transparently.

3. The principles

Article 5 of the UK GDPR relates to processing of personal data. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- 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 ('integrity and confidentiality')

4. Data Protection Officer

4.1 Requirement & Role

Under the DPA, a charity organisation should have a Data Protection Officer. A summary of the responsibilities of this role are set out below:

- Inform the controller (the Lighthouse Church), and its staff who carry out processing, of their obligations pursuant to this Regulation.
- Monitor compliance with this Regulation and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities awareness – raising and training of staff involved in processing personal data.
- Co-operate with the supervisory authority (Information Commissioner)
- Act as the contact point for all issues relating to the processing of personal information.

4.3 Training and Awareness

TLHC is committed to ensuring that all staff and volunteers are trained in their duties and responsibilities regarding the handling and security of personal information. To achieve this, we have implemented a comprehensive data protection training programme:

TBC if the below can be implemented:

- All new staff and volunteers will undertake data protection training upon joining the church.
- All existing staff and volunteers will be required to complete data protection refresher training approximately every 12 months.
- Different levels of training are provided based on the roles and responsibilities of the staff and volunteers.

This programme ensures that everyone within our community is aware of their obligations and understands the importance of protecting personal data in accordance with GDPR regulations.

5. Security and Information We Hold

5.1 Privacy Notice

TLHC's privacy notice is available on our website. In addition, we have a process in place to ensure that fair processing of information is always carried out when personal information is collected from individuals.

THLC's privacy notices will:

- Include details regarding the organisation and contact information for the church's Data Protection Officer.
- Be accessible, transparent, and written in plain English so they are easily understood.
- Contain sufficient detail to make it clear to individuals that the collection, processing, and purpose of personal data concerning them is explicit and legitimate.
- Include details of the rights of individuals and how they can exercise those rights.
- Confirm that data will only be kept for as long as necessary.

6. Rights of Individuals

6.1 Summary of Rights

The Data Protection Act provides several rights for individuals, as summarised below:

- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Data Portability
- Rights to Object
- Automated Decision making
- Compensation

6.2 Right of Access (Subject Access Request)

All individuals have a right of access to their own personal information. Any request by an individual for access to their own information must be considered a Subject Access Request. All requests for personal information will be managed by the Data Protection Officer to ensure that statutory deadlines are achieved.

7. Legal Basis for Processing Personal Data

7.1 Lawful Processing

We will only process personal data if at least one of the following applies:

- a. **Consent:** The individual has given explicit permission for their personal data to be processed for a specific purpose. Consent must be freely given, specific, informed, and unambiguous.
- b. **Contract:** Processing is necessary to fulfil a contract with the individual or to take steps at their request before entering a contract.
- c. **Legal Obligation:** Processing is necessary to comply with a legal obligation to which the organisation is subject. This excludes contractual obligations.
- d. **Vital Interests:** Processing is necessary to protect the vital interests of the individual or another person. This generally applies in life-or-death situations.

- e. **Public Task:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation.
- f. **Legitimate Interests:** Processing is necessary for the legitimate interests pursued by the organisation or a third party, provided these interests are not overridden by the individual's rights and freedoms. This basis is flexible but requires careful consideration and justification.

7.2 Statutory Obligations

All processing of personal data to conduct any statutory obligation will be undertaken in compliance with the requirements of the relevant legislation governing the statutory obligation and the principles of the DPA.

7.3 Consent

If consent is relied upon to process personal data, then this must be a freely given, specific, informed, and unambiguous statement of the data subjects agreement to the processing. Consent will not be assumed to be provided by silence or a non-response to a request.

The consent will be recorded in writing or by electronic means. If a verbal consent statement is unavoidable, it will be recorded and witnessed for future review.

7.4 Processing of Children's Data

Specific protection of the personal data relating to children is essential as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Such specific protection will particularly apply to the use of personal data for the purposes of marketing or creating personality or user profiles; for example in the collection and processing of personal data for use in relation to services being offered directly to a child (e.g. leisure), and parental consent will be sought where it is appropriate to do so, based on the service and/or the age of the child.

7.5 Retention

In some instances, the law sets the length of time information must be kept. In most cases, however, we use our discretion to ensure we do not keep records for longer than necessary.

8. International transfers

Where regular transfers of personal data are required outside of the UK, suitable international transfer agreements will be set up. Measures will be put in place to protect all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

9. Breaches and / or Complaints

If any potential breach of the DPA is suspected or identified, the Information Security Incident Response Procedure will be followed. Any complaint received regarding the council's handling of personal data should be directed to the Data Protection Officer (contact details in 4.2 above).

10. Record of Processing Activity (ROPA) – this will need be created

TLHC has identified its data processing activities by mapping out its key information assets on a central Record of Processing Activity (ROPA).

11. Data Minimisation

TLHC will identify and collect the minimum amount of personal data it needs to fulfil its purposes.

