ENFIELD TOWN COMMUNITY CHURCH

DATA PROTECTION POLICY

December 2024

Next review date: December 2025

Introduction

This document sets out the standards that the Trustees (the Elders) of Enfield Town Community Church ("the Church") expect to be adhered to by anyone who is dealing with personal information on behalf of the Church.

It should be read and followed by all members of staff and leaders of activities / groups who hold personal information.

It is important that the Church complies with Data Protection Legislation, not simply as a legal necessity (Romans 13:1 – "Let everyone be subject to the governing authorities…") but also to protect and love the individuals who come into contact with the Church, and, most importantly, to protect the name and honour of the Lord Jesus Christ.

The attached supporting documents form part of the overall Data Protection Policy:

- Appendix A – Retention of Records Policy
- Appendix B – Information Security Policy
- Appendix C – Church Data Breach Procedure
- Appendix D – Church Data Protection Compliant Process

Data Protection Legislation

The Data Protection Legislation ("the Legislation") means the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR). It confirms that everyone responsible for using personal data has to follow strict rules called 'data protection principles', which ensure the privacy of individuals is respected. In summary, these mean that they must make sure information is used:

- Fairly
- Lawfully and
- Transparently

This also includes any replacement data protection legislation relating to the Processing of Personal Data, including the guidance and codes of practice issued by the Information Commissioner's Office (ICO).

Data Protection at ETCC

During the course of its activities, the Church will collect, store and process personal data about our Members, people who attend our services and activities, 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 Church Secretary is responsible for ensuring compliance with the Legislation and with this Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred to the Church Secretary.

Compliance with the Legislation

Employees and others who process data on the Church's behalf 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 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 used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected)
- Be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction

The legal bases most frequently used by the Church for processing data are "Legitimate Interest" and "Consent". "Legitimate Interest" covers all data that we need to hold to run the Church and pastor the congregation effectively, such as holding personal details in order to be able to contact people quickly and easily.

"Consent" covers information held on those who do not attend the Church regularly but who wish to receive e-mails and other communications from the Church. Where "Consent" is used as the legal basis for processing data, it must involve some form of positive step by the individual to confirm their consent (such as actively ticking a box) and it must be possible for individuals to withdraw their consent at any time without any detriment to them, other than the Church not communicating with them any further.

Processing personal data

All personal data should be processed in accordance with the Legislation and this Policy. Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying personal data.

Personal data is data relating to a living individual who can be identified from that data or that data plus other information in the Church's possession. It includes identifiable images and 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 processed by the Church include:

- Names and addresses and other contact details of Church Members and others attending our services and other activities
- Pastoral records and notes, which may be sensitive in nature
- Employee details, including employment records
- Supplier details
- Recorded information including recorded telephone conversations, emails, photographic / video /CCTV images

Employees and others who process data on behalf of the 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
- It is necessary for the effective operation of the church and pastoring of the congregation, or
- 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 Church Secretary before processing personal data.

Monitoring the use of personal data

The Church is committed to ensuring that this Data Protection Policy is put into practice and that appropriate working practices are being followed. To this end:

- Any employees or Church volunteers who deal with personal data are expected to be aware of data protection issues.

- Those who handle personal data on a regular basis or who process sensitive or other confidential personal data have particular responsibilities to follow this Policy.

- All employees or Church volunteers who deal with personal data must evaluate whether the personal data they hold is being processed in accordance with this Policy. They have a responsibility to ensure inaccurate, excessive or out of date data is disposed of in accordance with this Policy.

- Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

The 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. Personal data stored on a computer / laptop should be password protected and not accessible to other users of the device. Shared email accounts should not be used to distribute / process personal information.

Data protection 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 the Church's behalf will be bound to comply with this Data Protection Policy.

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 (formally known as a subject access request) should be made to the Church Coordinator in writing, via the Church Office. In accordance with the Legislation, the Church 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

The Church reserves the right to change this Policy at any time. Where appropriate, it will notify data subjects of changes

Appendix A

ENFIELD TOWN COMMUNITY CHURCH

RETENTION OF RECORDS POLICY

Introduction

Data should only be kept as long as is necessary. This Policy sets out how long different types of data should be kept, how it will be shared and how it should be deleted.

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.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

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. 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".

7. Any data that is to be disposed must be safely disposed of for example by shredding.

8. Special care must be given to disposing of data stored in electronic media.

Data Retention Periods

Type of Data	Retention Period
Church Member information	Checked for accuracy annually Name and record of membership kept permanently; other information kept for up to two years after leaving membership
Details of regular attendees and other contacts (non-Members)	Checked for accuracy annually Removed within two years of contact ceasing
Information about children	Checked for accuracy annually Removed if a child does not attend a Church group / activity for a year, unless their parent/carer is a Member or regular contact Details of non-Members' children who are not themselves attending will be deleted during the summer after they turn 18 Details of children of Members will be kept in the prayer diary until they are approximately 21
Employment records	Six years after post-holder leaves ETCC employment
Financial records	Six years from the end of the relevant financial year Church Annual Accounts and Reports are kept permanently
Accident reports	Three years

Appendix B

ENFIELD TOWN COMMUNITY CHURCH

INFORMATION SECURITY POLICY

This Policy sets out the way in which the Church will preserve confidentiality, prevent unauthorised access, maintain integrity and safeguard the accuracy of information within the Church data.

Information security is the responsibility of every member of staff, Church Member and volunteer using Church data on, but not limited to, the Church information systems. The Church's IT systems may only be used for authorised purposes.

This Policy is the responsibility of the Church Secretary who will undertake supervision of the Policy.

The Church will ensure information security by:

- Ensuring appropriate software security measures are implemented and kept up to date
- Making sure that only those who need access have that access
- Not storing information where it can be accidentally exposed or lost
- Making sure that if information has to be transported it is done so safely using encrypted devices or services.

Access to IT systems on which personal information is stored must be password protected. Passwords must not be disclosed to others. If you have a suspicion that your password has been compromised you must change it. Particular care should be taken to ensure confidentiality when Church data, particularly sensitive pastoral data, is stored or processed on personally owned devices.

Individuals must ensure that any personally owned devices which have been used to store or process Church data is disposed of securely. Software on personally owned devices must be kept up to date. Unsecured WiFi must not be used to process Church data.

All breaches of this Policy must be reported to the Church Secretary as soon as possible.

Appendix C

ENFIELD TOWN COMMUNITY CHURCH

DATA BREACH PROCEDURE

Introduction

This paper sets out the procedure to be followed to ensure a consistent and effective approach to data protection in the Church. It also outlines what should be done in the event of any incident affecting personal data or any breach in the Church's Data Protection Policy.

Scope

The procedure relates to all personal data held by the Church, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the Church. The objective 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.

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 the Church is responsible for reporting data breach incidents immediately to the Church Secretary, or in his absence, the Lead Pastor. 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 Church Secretary 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 external authorities 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. The Church Secretary 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

Notification

The Church Secretary, if appropriate in consultation with the Lead Pastor / other Elders / external advice, will determine who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner 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/report-a-breach/personal-data-breach/

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 Church Secretary will keep a record of all actions taken in respect of the breach.

Evaluation and response

Once the incident is contained, the Church Secretary will 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.

Appendix D

ENFIELD TOWN COMMUNITY CHURCH

DATA PROTECTION COMPLAINT PROCESS

Introduction

This document sets out the process that an individual should follow if they have a complaint about the way their personal data has been handled. It links closely to the Church's Data Breach Procedure (Appendix C).

How to raise a complaint

The Church takes all data protection and privacy concerns seriously. If you have any concerns about the way your personal information is being handled, please contact the Church Secretary via the Church Office as soon as possible.

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 about data protection and data privacy should be raised with the Church Secretary as soon as possible, 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 if action needs to be taken in accordance with the Church's 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 Church Secretary will reflect on the circumstances and recommend any improvements to the Church's data protection systems or procedures.