



Corringham Evangelical Church

DATA PROTECTION POLICY

Last reviewed: January 2018
To be reviewed: January 2019

45 Fobbing Road, Corringham, Stanford-le-Hope, Essex, SS17 9BN
01375 642759 • www.corringhamevangelical.co.uk

Introduction

Corringham Evangelical Church collects and uses personal information about leaders, church members, and other individuals who come into contact with the church. This information is gathered in order to enable it to provide appropriate support. In addition, there may be a legal requirement to collect and use information to ensure that the church complies with its statutory obligations.

Churches have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All church members involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

The church is committed to maintaining the above principles at all times. Therefore the church will:

- Inform individuals why the information is being collected when it is collected;

- Inform individuals when their information is shared, and why and with whom it was shared;
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- Ensure church members are aware of and understand our policies and procedures.

Complaints

Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Church Oversight.

Contacts

If you have any enquires in relation to this policy, please contact David Partridge who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendix 1

Procedures for responding to subject access requests made under the Data Protection Act 1998:

Rights of access to information

Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to David Partridge. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out. Evidence of identity can be established by requesting production of:
 - a. Passport
 - b. Driving licence
 - c. Utility bills with the current address
 - d. Birth or Marriage certificate
 - e. P45/P60
 - f. Credit Card or Mortgage statement(This list is not exhaustive)
3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request.
4. The church may make a charge of up to £10 for the provision of information.
5. The response time for subject access requests, once officially received, is 40 calendar days. However the 40 days will not commence until after receipt of fees or clarification of information sought.
6. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.
7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the individual should not be disclosed.
9. If there are concerns over the disclosure of information then additional advice should be sought.
10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies/procedures then please contact David Partridge.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.