Romford Evangelical Free Church

DATA PROTECTION POLICY

Note: "Data Protection Legislation" means the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the Data Protection Act 2018 - the UK's implementation of the General Data Protection Guidelines (GDPR), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, 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 and the control of ways that personal information is used by organisations, businesses or the government. 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 Romford Evangelical Free Church ("the Church"), the Church Officers (Trustees, Deacons or other Ministry Leaders) will collect, store and process personal data about **members, people who attend services and activities, suppliers and other third parties.** It is recognised that the correct and lawful treatment of this data will maintain confidence in the Church. This policy sets out the basis on which the Church will process any personal data collected from data subjects, or that is provided by data subjects or other sources.

The Data Protection Officer is responsible for ensuring compliance with the Legislation and with this policy. The post is currently held by Janet Shaw (December 2019). Contact details are Romford Evangelical Free Church, 180 Brentwood Road, RM1 2RT, telephone 01708 769868.

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 Officer.

Changes to this policy

The Church reserves the right to change this policy at any time. Where appropriate, data subjects will be notified of those changes by mail or email.

The Policy includes paragraphs describing the following aspects: Page Nos below

Data Protection Policy adopted on 16/01/20……..
(Date of Church Trustees Meeting)

Due for Review on January 2021……..…

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Personal data is information relating to a living individual that enables them to be identified. It includes data about employees and volunteers as well as data collected as a result of church activities such as 'Messy Church'. 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, date of birth or email address) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details such as employment records, names and addresses, or other information about individuals, including supplier details, any third party data, and any recorded information including any recorded telephone conversations, emails or CCTV images.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data. This may be wholly or partly by automated means, or by other types of processing if it forms part of or is intended for any type of filing system.

Employees and volunteer "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. They should only process data if they have consent or a lawful basis for processing personal data:

- **Consent** of a data subject to the processing of their personal data
- **Contractual necessity**, when processing is needed for entering into or managing a contract (eg. as part of the employer/employee relationship such as processing the payroll)
- **Legal obligations** of the Data Controller
- **Vital interests**, such as specific data processed for matters of life and death
- **Public interest**, such as public authorities and organisations in the scope of their public duties and interest
- **Legitimate interests,** such as a weighed and balance legitimate interest where processing is needed and the interest is not overridden by others.

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

Sensitive data

The Church will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such will only be held if the explicit consent of each employee or volunteer is obtained or if one of the other conditions for processing sensitive data is satisfied.

Compliance with the Legislation

Employees and others who process data on behalf of the Church have a responsibility for processing personal data in accordance with the Legislation. They must ensure that they comply with the 7 data protection principles in the Legislation. These state that personal data must:

1 be obtained and used fairly and lawfully

2 be obtained for specified lawful purposes and used only for those purposes

3 be adequate, relevant and not excessive for those purposes

4 be accurate and kept up to date

5 not be kept for any longer than required for those purposes

6 be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction

7a 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)

7b not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect 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 the following steps will be taken:

- any employees/ volunteers 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/ volunteers who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;

- All employees/ volunteers 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;

- Spot checks may be carried out;

- Reports on the level of compliance with, or variance from good data protection practices may be produced by the Data Protection Officer. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Retention and storage of data and records

Any data file or record that contains personal data of any form can be considered as confidential in nature. All data and records will be stored in accordance with the security requirements of the Legislation and in the most convenient and appropriate location having regard to:

- the **period** of retention required (not longer than necessary for purpose for which it was collected)
- the **frequency** with which access will be made to the record
- the **status** of the records, such as active, or no longer active due to their age or subject.
- the **sensitivity** and confidential nature of the recorded material

Any unnecessary data must be safely disposed of, for example by shredding. Special care must be given to disposing of data stored in electronic media, such as personal computers.

Guidelines for Retention of Personal Data (Note: this is not an exhaustive list)

Please contact the Data Protection Officer if you have any queries regarding retaining or disposing of data

Types of Data	Suggested Retention Period
Church member information	Check for accuracy once a year
Secure destruction of personal data other than name and fact of membership	Three years after ceasing to be a member
Record that an adult was a member	**Permanent**
Church group member information	Check for accuracy once a year
Record that adult was a member of group	**Permanent**
Information relating to children	Check for accuracy once a year
Record that child was a member of the group	**Permanent**
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment
Application forms / interview notes	Maximum 1 year from the date of interviews for those not subsequently employed. If employed, retain in personnel file
Wages and salary records	6 years from the tax year in which generated
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	As above
Statutory Sick Pay records and calculations	As above
Statutory Sick Pay (General) Regulations 1982	As above
Accident books, and records and reports if accidents (for Adults)	3 years after the date of last entry (or of individual incidents)
Accident books, and records and reports if accidents (for children)	3 years after the child attains 18 years
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 (Limitation period for personal injury claims)	3 years from date of leaving employment

Security for handling personal data

'Church data' means any personal data processed by or on behalf of Romford Evangelical Free Church, the "Church".

Information security for Church data 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.

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.

Paper-based manual records relating to church members, volunteers or staff will be kept secure in locked cabinets. Access to such records will be restricted and precautions will be taken to avoid data being accidentally disclosed.

The Church will ensure that employees/ volunteers and members who handle personal data are adequately informed and monitored. Any agent employed to process data on behalf of the Church will be bound to comply with this data protection policy by a written contract.

The Church will take particular care of sensitive data, and security measures will reflect the importance of keeping sensitive data secure.

The Church IT systems may only be used for authorised purposes, and this will be monitored from time to time.

The Church will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing by:

- Ensuring appropriate software security measures are implemented and kept up to date;
- Ensuring that Computer files are password protected and that physical security measures are in place to guard against unauthorised disclosure.
- 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.

Passwords must not be disclosed to others. If any data user has a suspicion that their password has been compromised they must change it.

Data users must ensure that any personally owned equipment which has been used to store or process Church data is disposed of securely. Software on personally owned devices must be kept up to date and unsecured wifi must not be used to process Church data.

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 disposal via specialist contractors.

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

All breaches of this policy must be reported to the Data Protection Officer or the Trustees. (See next page)

Data Breach Procedures

The Church holds and processes personal data that must be carefully protected. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, a detrimental effect on service provision, legislative non-compliance or financial penalties.

These procedures are designed to ensure a consistent and effective approach throughout the church and apply to all personal data held by the Church, regardless of format. They cover 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 Romford Evangelical Free Church is responsible for reporting data breach incidents immediately to the Data Protection Officer, or in their absence to the Trustees and the Church Office. 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
- The number of individuals whose data is affected

Containment and recovery

The Data Protection Officer will firstly 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 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 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

Notification
With appropriate advice, The Data Protection Officer / Trustees will decide who else 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 www.ico.org.uk/media/1536/breach_reporting.pdf

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.

Evaluation and response
The Data Protection Officer will keep a record of all actions taken in respect of the breach. Once the incident is contained, they will review 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.

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 should be made to Data Protection Officer / Trustees in writing. In accordance with the Legislation, the Church will ensure that valid written requests for access to personal data are completed within 30 days of receipt. The data subject will be given:
a) a description of 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) a copy of the information in an intelligible form.

Data Protection Complaints Process

Romford Evangelical Free Church take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the Data Protection Officer without delay by calling 01708 381658 or email to trustees@romford-evan.co.uk. The Church will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation.

Any complaint must be referred to The Data Protection 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 Procedures.
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 Office and the Trustees will reflect on the circumstances and recommend any improvements to systems or procedures.

If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/