SURREY CHAPEL DATA PROTECTION POLICY

"Data Protection Legislation"	means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), 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. 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 Surrey Chapel ("the Church"), the Church Trustees ("we") 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 Data Controller is the Church management Team who determine the purpose for which and the manner in which any personal data is processed

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. They can be contacted via email on dataprotection@surreychapel.org.uk

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 Compliance Manager.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy will be considered a serious matter. Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It include data about volunteers and any individual attending Surrey Chapel or any of its groups or activities. 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 are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third party data and any recorded information including any recorded telephone conversations, emails or CCTV images. It includes personal information such as email addresses and telephone numbers held to enable the Church to pursue its legitimate interests in accordance with its mission and aims

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
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll
- If it is necessary for a volunteer, group leader or any other individual to pursue the legitimate interests of Surrey Chapel
- If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees and others who process data on our 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 and lawfully
- 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
- 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

We are 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 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 who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All employees 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;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the Data Protection Compliance Manager. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

We 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. Computer files should be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security 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 our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop should be password protected.

The rights of individuals

Data Subjects are individuals about whom information is held. The Legislation gives these 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 the Church Administrator in writing. In accordance with the Legislation we 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.

Sensitive data

We 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 should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

Reviewed May 2019