GREENSTEAD EVANGELICAL FREE CHURCH

DATA PROTECTION POLICY

Data Protection Legislation was incorporated into the General Data Protection Regulation (GDPR), effective from 25 May 2018. Its purpose is the protection of human rights in relation to personal data, and to ensure that such data is used fairly and lawfully and that where necessary the privacy of individuals is respected. This document sets out how Greenstead Evangelical Free Church ('the Church" or "we") uses data provided by complying with all relevant laws and adopting good practice. The Church is committed to protecting all information that we handle about people we support and work with, and to respect people's rights around how their information is hand. This policy explains our responsibilities and how will meet them, together with explanations as to the personal data held on an individual, how we collect it, why we collect it, the legal bases by which we process the data, and how we protect and store it. It also explains the rights of individuals under GDPR.

We have considered whether the Church has an obligation to appoint a Data Protection Officer. On the basis of guidance from the Information Commissioners Office (ICO) we do not consider such an appointment is necessary. However, the Trustees of the Church are responsible for advising the Church and its staff and members about their legal obligations under the data protection law, monitoring compliance with such law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at pastor@gefc.org.uk

1. What data we collect.

From individuals we collect personal information which may be factual such as names, addresses, telephone and mobile numbers and email addresses, but may also collect information which can be an opinion about that person, their actions and behaviour. We also collect employee data. We may also collect data from suppliers.

In some cases we may hold types of information that are called "special categories" of data in the GDPR. This includes information about a person's: racial or ethnic origin; political opinions religious or similar beliefs; trade union membership; health (including physical and mental health and the provision of healthcare services); genetic data; biometric data; sexual life and sexual orientation. These items of data can only be processed under strict conditions.

We will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data, such as where it fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk or one of the additional conditions relating to criminal convictions set out in legislation.

2. How we collect data.

Data is collected personally from an individual, normally when they become an employee or a member of the Church. On occasions information will be provided by other individuals who may be members of the congregation or attend meetings organised by the Church.

3. Why we collect data.

We collect and use your personal data:

- to maintain our list of church members and regular attendees,
- to send communications regarding the various activities of the church,
- to provide appropriate pastoral care and support for members and others connected with the church,
- to provide services to the community including mother and toddler groups and 'drop in' groups,
- to safeguard children, young people and adults at risk,
- to monitor and assess the quality of our services,
- to maintain our accounts and records,
- to respond effectively to enquiries and handle any complaints.

4. Legal bases by which we obtain data.

In accordance with GDPR we will ensure that all personal data:

- is obtained and processed fairly, lawfully and in a transparent manner:
- is obtained and processed for specified, explicit and legitimate purposes and used only for those purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- be accurate and kept up-to-date;
- not be kept longer than necessary the purposes for which it is being processed;
- be processed in a secure manner by using appropriate technical and organisational means;
- be processed in keeping with the rights of data subjects regarding personal data.

5. How we process (use) data.

We process data for the reasons given in (3) above. Processing has to be fair and lawful and this is achieved when it meets a legal basis and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them as well as when we collect data about them from other sources.

The processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

- the processing is necessary for a contract with the data subject;
- the processing is necessary for us to comply with a legal obligation;
- the processing is necessary to protect someone's life (this is called "vital interests");
- the process is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
- the processing is necessary for legitimate interests pursued by Greenstead Evangelical Free Church or other organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

If none of the above legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

Processing of "special categories" (as detailed in (1) above) is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in article 9 of the GDPR, is met. These conditions include where:

- the process is necessary for carrying out our obligations under employment and social security and social protection law;
- the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and this data subject is incapable of giving consent;
- the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes as a church;
- the processing is necessary for pursuing legal claims.

If none of the above legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

6. How we protect data.

We will use appropriate measures to keep personal data secure at all points of the processing. This involves preserving confidentiality, unauthorised access, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users. Also includes protecting it from accidental loss, destruction or damage.

Information security is responsibility of every member of staff, trustee, officeholder church member or volunteer using Church data but not limited to the Church information systems. This policy is responsibility of the Trustees who will undertake supervision of the policy.

Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time and any person using them for unauthorised purposes may be subject to disciplinary and/or legal proceedings. We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- all manual (written) records will be securely stored in lockable cupboards at the church premises and access will be restricted;
- access to systems on which information is stored must be password protected with strong passwords and these should be changed immediately if there is a risk they have been compromised. Access will be restricted and passwords must only be disclosed to authorised persons;
- we will ensure that persons authorised to handle personal data are adequately trained and monitored to ensure that it is being kept secure and that access to data will only be made available to those who have a clear requirement for such access ;
- we will take particular care of sensitive data and security measures will reflect the importance of keeping this 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 backup files from IT systems and the 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.
- where personal devices are used to store or process personal data, they must be subject to appropriate security.

7. How we store data and how long it is retained.

All data and records will be stored in accordance securely 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.

Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements. 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 or destroyed. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. Any data file or record which contains personal data of any form can be considered as confidential in nature.

Data and records should not be kept for longer than is necessary for that purpose. All staff, trustees, volunteers and members of the Church are required to have regard to the Guidelines for Retention of Personal Data below which are attached at the end of this document.

Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the Minister who will undertake secure shredding.

Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Church Leadership team to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of.

8. Data breaches.

The policy on data breaches relates to all personal data held by the Church, regardless of how the data is held, and applies to *anyone* who handles this personal data, including those working on behalf the Church.

A potential breach 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. Examples of such an event are loss, theft or failure of equipment on which personal data is stored, unauthorised or attempted unauthorised access to personal data, unauthorised disclosure of personal data, or a hacking attempt.

Any person using personal data on behalf of the Church and who becomes aware of a potential breach must immediately notify the Minister, or in his absence the trustees, the date and time of discovery of the breach, details of the person who discovered it, the nature of the data involved and how many individuals' data is affected. The Pastor will ascertain if the breach is still continuing and if appropriate take steps immediately to minimise the effects. An assessment will be carried out to established the severity of the breach and consideration given as to whether police should be informed.

Records of any personal data breaches must be maintained and if they are likely to result in a risk to any person, they must be reported to the Information Commissioners Office within **72** hours of any person becoming aware of the breach. If a personal data breach causes a

high risk to any person we will (as well as reporting the breach to the ICO), inform the data subject whose information is affected without undue delay. This can include situations where, for example, bank details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

9. Data subjects' rights.

We will process personal data in line with data subjects' rights, including their right to:

- request access to any of their personal data held by us (known as a Subject Access Request);
- ask to have inaccurate personal data changed;
- restrict processing, in certain circumstances;
- object to processing, in certain circumstances;
- data portability, which means to receive their data, or some of their data, in a format that can easily be used by another person (including the data subject themselves) or organisation;
- not to be subject to automated decisions, in certain circumstances;
- withdraw consent when we are relying on consent to process their data.

Any request from a data subject that relates or could relate to their data protection rights should be forwarded to the Minister, or in his absence the trustees, **immediately.** Any valid request should be acted as soon as possible, and at the latest within **one calendar month,** unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

All of the above rights are provided free of charge and information provided shall be concise and transparent, using clear language.

10. Complaints.

If you have any concerns about the way your information is being handled, please contact the Minister who can be contacted by telephone on 01206 510114 or email at pastor@gefc.org.uk

We will carefully investigate and review all complaints and take appropriate action, and will keep you informed of the progress 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/concerns/

11. Changes to this policy.

We reserve the right to change this policy at any time, including as needed to comply with changes in law. Where appropriate we will notify data subjects of these changes by post or email. This document will be reviewed every 12 months.

Policy adopted by the Trustees on 11 July 2018.