Data Protection Policy

May 2017

CONTENTS

CLAUSE

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that Church Army ("We") may be required to handle include information about our current, past and prospective Commissioned Evangelists and employees; our volunteers; those for whom we provide care; our donors; our guests; our suppliers, contractors and other third parties. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations ("the Regulations").

2.2 This policy and any other documents referred to in it 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.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 In addition, occasionally we may be required by law to collect and use certain types of personal data to comply with the requirements of government departments.

2.5 This policy has been approved by the Management Team of Church Army. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer, store and destroy personal data.

2.6 The Deputy Chief Executive, Des Scott, has responsibility for any issues surrounding data protection within the organisation and he is responsible for ensuring compliance with the Regulations 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 in the first instance to Des Scott.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is recorded and processed electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). 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.

3.4 **Data controller** is the person (either alone or jointly or in common with other persons) who determines the purposes for which and the manner in which any personal data are, or are to be processed. We are the data controller of all personal data used in our organisation.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this Data Protection Policy and any applicable data security procedures at all times.

3.6 **Data processors** are any persons (other than an employee of the data controller) who processes the data on behalf of the data controller, so any person who processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, adaptation or alteration, retrieving, using, disclosing (by transmission, dissemination or otherwise making available), erasing, blocking or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of (or alleged commission), or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any Court in such proceedings. Sensitive personal data can only be processed under strict conditions.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the enforceable principles set out in Article 5 of the GDPR. These provide that personal data must be:

(a) Processed fairly, lawfully and in a transparent manner.

(b) Collected and processed for one or more specified, explicit and legitimate purposes and not further processed in any matter incompatible with that purpose(s).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) Accurate, and where necessary kept up to date, with every reasonable step being taken to erase or rectify without delay inaccurate data.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is being processed, subject to appropriate technical and organisational measure, to safeguard the rights and freedoms of individuals.

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

(g) Processed in accordance with the accountability principles set out in Article 5 (2) of the GDPR stating we are explicitly responsible for demonstrating that we comply with the principles.

5. FAIR AND LAWFUL PROCESSING

5.1 The Regulations are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in Article 6 (1) of the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject or to enter into a contract, for the compliance with a legal obligation to which the data controller is subject, for the legitimate interest of the data controller or the party to whom the data is disclosed.

5.3 When sensitive personal data is being processed, one of the additional conditions (set out in Article 9 (2) of the GDPR) must be met, including among other things explicit consent, in order to comply with employment law or if the processing is carried out in the course of the legitimate activities of a not-for-profit body and where the processing relates to personal data which is manifestly made public by the data subject, as well as for the establishment, exercise or defence of legal claims.

When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, telephone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in our notification to the Information Commissioner or for any other purposes specifically permitted by the Regulations. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter, at all times being open about our reasons for collecting the data.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data, including their right to withdraw consent for us to use their personal data at some point in the future.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter and by no later than one calendar month.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND LIMITED TO THE PURPOSES PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, so data that is sufficient for the purpose we are holding it for. We will not hold more information than we need for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

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

(a) Request access to any data held about them by a data controller, known as a subject access request. (see also clause 16).

(b) To be forgotten, to restrict and object to processing, through erasure or quarantine.

(c) Data portability, allowing individuals to request their data in a machine-readable format. Individuals can also ask for the data to be transferred directly from one controller to another.

(d) To object to direct marketing.

(e) Not be subject to decisions made automatically that produce legal effects or significantly affect the individual. To protect against the risk of a potentially damaging decision being taken without human intervention.

(f) Ask to have inaccurate data amended, blocked, erased or destroyed. (see also clause 9).

(g) To withdraw consent for us to process their data, at any time.

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss or destruction of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

12.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Services Manager.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.) Desks should be clear of any personal information not being processed at the time.

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

(e) **System access.** Only those data users or data processors who require access to the data will have access, through restricting access both on the computer systems and to paper files and documents.

13. DATA PROCESSORS

Any data processor employed by us to process personal data on our behalf should only do so on our documented instructions. The Regulations place an obligation on the parties to ensure there is a proper processing contract in place between the data controller and the data processor, to reflect their joint liability to comply with the Regulations.

When instructing a data processor to process data on our behalf a written contract needs to be entered into which sets out the scope, nature and purposes of the processing, the duration of the processing and the types of personal data and categories of data subjects. All processors should be carefully vetted and selected to ensure they can meet all the requirements of the Regulations.

A copy of any new contract entered into needs to be passed to Des Scott to be held on the organisation's central data protection records.

14. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

14.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent (which must be explicit and subject to certain limitations set out in the Regulations).

(c) The transfer is necessary for one of the reasons set out in the Regulations, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

14.2 Subject to the requirements in clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

15.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

15.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

15.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15.4 We may also share personal data we hold with selected third parties for the purposes set out in our notification to the Information Commissioner.

16. DEALING WITH SUBJECT ACCESS REQUESTS

16.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to Des Scott immediately, as all such requests have to be responded to within a month (2 months in more complex cases).

16.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

16.3 Our employees will refer a request to their line manager or to Des Scott for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

17. DATA PROTECTION BREACHES

A data protection breach would include the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data, which contains a risk to a data subject.

In the unlikely event of a data protection breach in accordance with the Regulations we will notify the Information Commissioner within 72 hours of becoming aware of the breach. If the breach contains a high risk to the data subject(s) concerned, we will notify them immediately of the breach. All breaches and potential breaches should be notified to Des Scott with immediate effect in order that they can be responded to in accordance with the regulations.

We will take all reasonable steps to minimise the impact and consequences of a breach, in conjunction with guidance from the Information Commissioner.

18. 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.