

RESOURCE FOR ANGLICAN RENEWAL MINISTRIES

DATA PROTECTION POLICY

CONTENTS

Clause Heading	Page
1 Policy Statement	1
2 About this Policy	1
3 Definition of Data Protection Terms	1
4 Data Protection Principles	3
5 Fair and Lawful Processing	3
6 Processing for Limited Purposes	3
7 Notifying Data Subjects	4
8 Adequate, Relevant and Non-excessive Processing.....	4
9 Accurate Data.....	4
10 Timely Processing	4
11 Processing in Line With Data Subject's Rights.....	5
12 Data Security.....	5
13 Transferring Personal Data to a Country Outside the Eea	6
14 Disclosure and Sharing of Personal Information	6
15 Dealing With Subject Access Requests.....	7
16 Changes to this Policy	7
The Schedule Data Processing Activities	8

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 about our supporters, donors, employees, volunteers, service users, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.
- 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 we may be required to handle include information about current, past and prospective suppliers, donors, employees, volunteers, service users and others that we communicate with. 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 Data Protection Act 1998 (the Act) and other 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 This policy has been approved by the Board of Trustees. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.
- 2.5 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Mrs Lydia Farnham, office@resource-arm.net, 01952 371300. 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.

3 Definition of Data Protection Terms

- 3.1 **Data** is information which is stored 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 controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our organisation for the organisation's purposes.
- 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** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
- 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, amending, retrieving, using, disclosing, erasing 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 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, including a condition requiring the express permission of the person concerned.

4 Data Protection Principles

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

4.1.1 processed fairly and lawfully;

4.1.2 processed for limited purposes and in an appropriate way;

4.1.3 adequate, relevant and not excessive for the purpose;

4.1.4 accurate;

4.1.5 not kept longer than necessary for the purpose;

4.1.6 processed in line with data subjects' rights;

4.1.7 secure; and

4.1.8 not transferred to people or organisations situated in countries without adequate protection.

5 Fair and Lawful Processing

5.1 The Act is 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, they must be processed on the basis of one of the legal grounds set out in the Act. 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, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our operations, 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 the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data

we receive from other sources (including, for example, 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 the Schedule or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7 Notifying Data Subjects

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

7.1.1 the purpose or purposes for which we intend to process that personal data;

7.1.2 the types of third parties, if any, with which we will share or to which we will disclose that personal data; and

7.1.3 the means, if any, with which data subjects can limit our use and disclosure of their personal data.

- 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.

- 7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Compliance Manager is.

8 Adequate, Relevant and Non-excessive Processing

- 8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9 Accurate Data

- 9.1 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

- 10.1 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

- 11.1 We will process all personal data in line with data subjects' rights, in particular their right to:
 - 11.1.1 request access to any data held about them by a data controller (see also clause 15);
 - 11.1.2 prevent the processing of their data for direct-marketing purposes;
 - 11.1.3 ask to have inaccurate data amended (see also clause 9); and
 - 11.1.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

12 Data Security

- 12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss 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:
 - 12.3.1 **confidentiality** means that only people who are authorised to use the data can access it;
 - 12.3.2 **integrity** means that personal data should be accurate and suitable for the purpose for which it is processed; and
 - 12.3.3 **availability** means that authorised users should be able to access the data if they need it for authorised purposes.
- 12.4 Security procedures include:
 - 12.4.1 **entry controls**. Any stranger seen in entry-controlled areas should be reported;

- 12.4.2 **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);
- 12.4.3 **methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required; and
- 12.4.4 **equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13 Transferring Personal Data to a Country Outside the EEA

- 13.1 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:
 - 13.1.1 the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;
 - 13.1.2 the data subject has given his consent;
 - 13.1.3 the transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;
 - 13.1.4 the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; and
 - 13.1.5 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.
- 13.2 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.

14 Disclosure and Sharing of Personal Information

- 14.1 We may also disclose or share personal data 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 organisations for the purposes of fraud protection and credit risk reduction.

- 14.2 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

15 Dealing With Subject Access Requests

- 15.1 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 the Data Protection Compliance Manager immediately.

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

15.2.1 we will check the caller's identity to make sure that information is only given to a person who is entitled to it; and

15.2.2 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.

- 15.3 Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16 Changes to this Policy

- 16.1 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.

The Schedule
Data Processing Activities

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Retention period
Name Contact details Financial contributions Subscriptions Purchases Details of events attended	Supporters	Processed on a password protected database which is managed remotely by GJ Stats Gift Aid and standing order mandate forms kept in a locked cabinet or drawer in office which is kept locked by key code	To keep supporters updated and supplied with news etc. To enable accurate distribution of resources For planning purposes To keep accurate individual financial records	Trustees (electronic) Director Core team members (electronic)	Keep on the database indefinitely if a regular donation is being received Financial data for at least 6 years Gift Aid forms for 6 years after the last donation or the relevant period Where there is no financial information - when asked by data subject to have information removed
Name Contact details Financial contributions Subscriptions Purchases	Donors	Processed on a password protected database which is managed remotely by GJ Stats Gift Aid and standing order mandate forms kept in a locked cabinet or drawer in office which is kept locked by key code	To keep donors updated and supplied with news etc. To enable accurate distribution of resources For planning purposes To keep accurate individual financial records	Trustees (electronic) Director Core team members (electronic)	Keep on the database indefinitely if a regular donation is being received Financial data for at least 6 years Gift Aid forms for 6 years after the last donation
All personal details collected on application Proof of ID and right to work in UK Bank details Tax details	Employees	Kept on password protected PC Kept in locked cabinet in locked storage room	Legal requirements for employment and payment of salaries	Trustees Director Accountants	Job applications - 6 months Tax details – 6 years Contract of employment claims – 6 years Disciplinary information – 6 months

Pension details Disciplinary details Sick certificates Health & safety information					Health or personal injury information – 3 years Pension details - indefinitely
Name Contact details Health & safety information (if & when an incident occurs)	Volunteers	On password protected computer	To enable contact and for record keeping	Director	For as long as the volunteer is working with us Health & Safety information – 3 years
Name Contact details Details of service used	Service users (attendees of our events)	Processed on a password protected database which is managed remotely by GJ Stats	For record keeping	Trustees Director Core team	When asked by data subject to be removed from our records