Data Protection Policy

Payroll Giving in Action Ltd

1. Purpose of the policy

1.1 Payroll Giving in Action Ltd is committed to complying with privacy and data protection laws including the Data Protection Act 1998 (**"the DPA"**). This policy sets out what we do to protect individuals' personal information.

1.2 Anyone who handles personal data in any way on behalf of Payroll Giving in Action Ltd must ensure that they comply with this policy. Section 3 of this policy describes what comes within the definition of "personal data". Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.3 This policy may be amended to reflect any changes in legislation, regulatory guidance or internal policy decisions. You may not necessarily be notified of these changes so you should review the policy from time to time.

2. About this policy

2.1 The types of personal information that we may handle include details of: Payroll Giving donors.

2.2 Jeremy Colwill is responsible for ensuring compliance with the DPA and with this policy. Any questions or concerns about this policy should be referred in the first instance to Jeremy Colwill, who can be contacted at jcolwill@payrollgiving.co.uk or on 01271 344360.

3. Definitions of data protection terms

The following terms will be used in this policy and are defined below:

3.1 **data subjects** 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 data.

3.2 **personal data** means information relating to a living person who can be identified from that information (or from that information when combined with other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.3 **data controllers** are the people who, or organisations which, decide the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to process personal data in compliance with the DPA. **Payroll Giving in Action Ltd is the data controller of all personal data that we manage in connection with our work and activities.**

3.4 **data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website or server hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.5 **EEA** is the European Economic Area which includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.6 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.7 **processing** is any activity that involves use of personal data. It includes obtaining, recording, holding, organising, amending, using, disclosing or destroying personal data.

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;
- sexual life or orientation; or
- criminal record (including any allegation that they have committed an offence).

4. Data protection principles

Anyone processing personal data must comply with the eight data protection principles. We are required to comply with these principles (summarised in paragraphs 5-11 below) in respect of any personal data that we deal with as a data controller.

Personal data should be:

4.1 processed fairly and lawfully;

4.2 processed for purposes which the individual has been told about, and not in any way that is incompatible with those purposes;

4.3 adequate, relevant and not excessive in relation to the purpose for which it is held;

4.4 accurate and, where necessary, kept up to date;

4.5 not kept longer than necessary;

4.6 processed in accordance with individuals' rights;

4.7 secure; and

4.8 not transferred to people or organisations outside the EEA without adequate safeguards.

5. Processing data fairly and lawfully

5.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about.

5.2 To do this, every time we receive personal data about a person, which we intend to keep, we need to provide that person with **"the fair processing information"**. In other words we need to tell them promptly:

5.2.1 who will be holding their information, i.e. Payroll Giving in Action Ltd;

5.2.2 why we are collecting their information and what we intend to do with it for instance to process donations or send them mailing updates about our activities; and

5.2.3 anything else necessary to make sure that we are using their information fairly, for example, if we plan to share their information with another organisation.

5.3 This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms.

5.4 Obtaining an individual's consent can help to ensure we process their data fairly but in most cases it is not required. Exceptions to this are covered in paragraphs 12 and 15 below.

6. Processing data for the original purpose

6.1 The second data protection principle requires that personal data is only processed for the specific purposes that the individual was told about when we first obtained their information.

6.2 This means that we should not collect personal data for one purpose and then use it for another, unless the second purpose is implicit.

7. Personal data should be accurate

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Inaccurate or out-of-date data should be archived if necessary or otherwise destroyed securely.

8. Not retaining data longer than necessary

8.1 The fifth data protection principle requires that we should not keep personal data for longer than we need it for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please speak to Jeremy Colwill.

8.2 For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please contact Jeremy Colwill or seek legal advice.

9. Rights of individuals under the DPA

The DPA gives people rights in relation to how organisations process their personal information. They include (but are not limited to) the right:

9.1 to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made

of the information and details of anyone to whom their personal data has been disclosed (known as subject access rights);

9.2 to have inaccurate data amended or destroyed.

9.3 to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else; and

9.4 to ask us to cease processing for direct marketing purposes.

10. Data security

10.1 The seventh data protection principle requires that we keep secure any personal data that we hold.

10.2 We are required to put in place procedures to keep the personal data that we hold secure.

10.3 When we are dealing with sensitive personal data (as defined in paragraph 3.8 above), more rigorous security measures are likely to be needed, for instance, if sensitive personal data is held on a memory stick or other portable device it should be encrypted.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures must be followed in relation to all personal data processed by us:

- Entry controls: Any stranger seen in entry-controlled areas should be reported;
- Equipment: Users should ensure that individual monitors do not show confidential information to others who are unauthorised and that they log off from their PC when it is left unattended;
- 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);
- Methods of disposal: Paper documents should be shredded. Memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required
- Backing up data: Daily back-ups should be taken of all data on our system; data should not be stored on local drives or removable media as these will not be backed up;
- Travelling with personal data and remote working: Staff must keep data secure when travelling or using it outside of our offices. For instance:
    - documents and laptops must be kept secure (not left lying around off site);

- where you are using media that contains suitable software, you should make every effort to arrange for encryption (Speak to Jeremy Colwill)

- data stored on computers when working at home must be password protected, and kept confidential;

- when you are working from home, you should ensure that the laptop or computer you are using is securely protected from theft while you are away from it.

- Secure exchange of data: Personal data must always be transferred in a secure manner. The degree of security required will depend on the nature of the data; the more sensitive and confidential the data, the more stringent the security measures should be. The following precautions should be taken:

    - use registered post or courier. Never send a CD or stick containing personal data by ordinary post;

    - use password protection (on files) if sending by email – but recognise this is not very secure and should only be used for small quantities of information;

    - never send sensitive data, by email unless it has been encrypted (speak to Jeremy Colwill for more details).

    - If you wish to process personal data on your personal device (such as a smartphone or tablet) you need to be satisfied that it is being processed securely. Please discuss this with Jeremy Colwill before doing so.

11. Transferring Data Outside the EEA

11.1 The eighth data protection principle requires that when organisations transfer personal data outside the EEA they take steps to ensure that the data is properly protected.

11.2 The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, and this list may be updated.

11.3 As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it may be necessary to seek the consent of the individuals whose data is being transferred or to enter into an EC-approved agreement.

11.4 For more information, please speak to Jeremy Colwill or seek further legal advice.

12. Processing sensitive personal data

12.1 On some occasions we may collect information about individuals that is defined by the DPA as **sensitive**, and special rules will apply to the processing of it. The categories of sensitive personal data are set out in the definition in section 3.

12.2 Purely financial information is not technically defined as sensitive personal data by the DPA, however, particular care should be taken when processing such data, as the ICO is likely to treat a breach relating to financial data very seriously.

12.3 In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

12.4 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the DPA permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to Jeremy Colwill.

13. Notification

13.1 Our data protection notification defines our data subjects (i.e. the people about whom we hold personal data), our data categories (the information we hold about them) and our purposes (the reasons why we hold this information). A copy of our notification may be viewed on request, or online via the public register on the web site of the ICO (www.ico.org.uk).

13.2 We should only engage in processing which comes within the categories set out in our Notification. Processing for additional purposes should not take place. The Notification is reviewed once every two years to ensure it is still accurate and up to date. If you think our Notification needs to be updated to include additional processing, please tell the Jeremy Colwill.

14. Consent

Whilst consent is not required to process most data, it is usually required to process sensitive personal data (see paragraph 12 above) and is normally required to send direct marketing by email or SMS. Please speak to Jeremy Colwill if you plan to do this.

15. Monitoring and review of the policy

This policy is reviewed Annually by our board of directors to ensure that it is achieving its objectives.