DATA PROTECTION POLICY

Young Friends General Meeting of the Religious Society of Friends

Including Privacy Policy

Contents

Based on a template prepared by:

Bates Wells Braithwaite

10 Queen Street Place, London EC4R 1BE

www.bwbllp com

1. Purpose of the policy

1.1 Young Friends General Meeting of the Religious Society of Friends is committed to complying with privacy and data protection laws including:

(a) the UK General Data Protection Regulation **("the UK GDPR")** and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017 and the Data Protection Act 2018.

(b) the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and

(c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO") or any other supervisory authority. (together "the Legislation")

1.2 This policy sets out what we do to protect individuals' personal data.

1.3 Anyone who handles personal data in any way on behalf of Young Friends General Meeting of the Religious Society of Friends must ensure that we 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.

1.4 This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

2. About this policy

2.1 The types of personal data that we may handle include details of: members of YFGM, including trustees, volunteers, and event participants; donors; and grant applicants and recipients.

2.2 The Management Trustee at Young Friends General Meeting of the Religious Society of Friends is responsible for ensuring compliance with the UK GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to the YFGM Coordinator who can be contacted at yfgm@quaker.org.uk or on 020 7663 1050, or to the Management Trustee who can be contacted at yfgm.management.trustee@quaker.org.uk.

3. Definitions of data protection terms

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

3.2 **Data Subjects** include all living individuals about whom we hold personal data, for instance an employee or a supporter. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and 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). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4 **Data Controllers** are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. Young Friends General Meeting of the Religious Society of Friends is the data controller of all personal data that we manage in connection with our work and activities.

3.5 **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 hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.6 **European Economic Area** includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

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

3.8 **Processing** is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

(a) collecting;
(b) recording;
(c) organising;
(d) structuring;
(e) storing;
(f) adapting or altering;
(g) retrieving;
(h) disclosing by transmission;
(i) disseminating or otherwise making available;
(j) alignment or combination;
(k) restricting;
(l) erasing; or
(m) destruction of personal data.

3.9 **Sensitive Personal Data (which is defined as "special categories of personal data" under the UK GDPR)** includes information about a person's:

(a) racial or ethnic origin;

(b) political opinions;

(c) religious, philosophical or similar beliefs;

(d) trade union membership;

(e) physical or mental health or conditions;

(f) sexual life or orientation;

(g) genetic data;

(h) biometric data; and

(i) such other categories of personal data as may be designated as "special categories of personal data" under the Legislation.

4. Data protection principles

4.1 Anyone processing personal data must comply with the six data protection principles set out in the UK GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any personal data that we deal with as a data controller.

4.2 Personal data should be:

(a) processed fairly, lawfully and transparently;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary for the purpose for which it is held;

(d) accurate and, where necessary, kept up to date;

(e) not kept longer than necessary; and

(f) processed in a manner that ensures appropriate security of the personal data.

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. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

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

(a) the type of information we will be collecting (categories of personal data concerned);

(b) who will be holding their information, i.e. Young Friends General Meeting of the Religious Society of Friends including contact details and the contact details of our Data Protection Officer (if we have one);

(c) 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;

(d) the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis);

(e) if we are relying on legitimate interests as a basis for processing what those legitimate interests are;

(f) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;

(g) the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;

(h) details of people or organisations; with whom we will be sharing their personal data;

(i) if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards; and

(j) the existence of any automated decision-making including profiling in relation to that personal data.

5.3 Where we obtain personal data about a person from a source other than the person themselves, we must provide that individual with the following information in addition to that listed under 5.2 above:

(a) the categories of personal data that we hold; and

(b) the source of the personal data and whether this is a public source.

5.4 In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights outlined in section 9 below, including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

5.5 This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

6. Processing data for the original purpose

6.1 The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate 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. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual's consent.

7. Personal data should be adequate and accurate

7.1 The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

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 to 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 The YFGM Coordinator.

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 The YFGM Management Trustee or refer to 2.7 of the Privacy Policy.

9. Rights of individuals under the UK GDPR

9.1 The UK GDPR gives people rights in relation to how organisations process their personal data.

9.2 Everyone who holds personal data on behalf of Young Friends General Meeting of the Religious Society of Friends needs to be aware of these rights. They include (but are not limited to) the right:

(a) 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, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);

(b) to be told, where any information is not collected from the person directly, any available information as to the source of the information;

(c) to be told of the existence of automated decision-making;

(d) to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;

(e) to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;

(f) to restrict processing where the individual has objected to the processing;

(g) to have inaccurate data amended or destroyed; and

(h) to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. Data security

10.1 The sixth 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, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.3 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always 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 and monitoring processes must be followed in relation to all personal data processed by us: backing up data (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up); staff should 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; paper documents should be shredded, memory sticks, CO-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required; 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); desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and staff must keep data secure when travelling or using it outside the offices.

11. Transferring Data Into and Out of the EEA

11.1 The UK GDPR requires that when organisations transfer personal data in or out of 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, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, New Zealand, Switzerland, Jersey, Uruguay and the United Kingdom. but 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 will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the UK GDPR that apply to the transfer of personal data outside the EEA.

11.4 Transfers to the USA; advice should be sought from the data protection officer (if we have one) before transferring personal data to organisations in the USA, these transfers should be Risk Assessed on an individual basis.

11.5 For more information, please speak to the YFGM Coordinator 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 UK GDPR as special categories of personal data, and special rules will apply to the processing of this data. In this policy we refer to "special categories of personal data" as "sensitive personal data". The categories of sensitive personal data are set out in the definition in Section 3.9.

12.2 Purely financial information is not technically defined as sensitive personal data by the UK GDPR. However, particular care should be taken when processing such data, as the ICO will 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 UK GDPR permits organisations to process sensitive personal

data, including where the processing is carried out in the course of YFGM's legitimate activities, as a body which is not established or conducted for profit and exists for religious purposes. 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 the YFGM Coordinator or the Management Trustee.

13. Notification

13.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the UK GDPR, we will consult with the ICO where necessary when we are carrying out "high risk" processing.

13.2 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

14. Record keeping

14.1 We must keep a record of our data processing activities, to demonstrate that we are complying with them. These records will include the purpose of processing, descriptions of categories of data subjects and categories of personal data, details of transfers to third countries and retention periods of personal data.

15. Monitoring and review of the policy

15.1 This policy is reviewed annually by our board of trustees to ensure that it is achieving its objectives.

Appendix 1 – Privacy Policy

Young Friends General Meeting (YFGM) is committed to complying with privacy and data protection laws.

1. What information do we collect?

1.1 Young Friends General Meeting may collect, use, and store the following personal data:

(a) information about your computer and about your visits to and use of this website (including your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths);

(b) information that you provide to us for the purpose of registering for YFGM events, including but not limited to your name, telephone number, email address, and postal address;

(c) information that you provide to us for the purpose of receiving communications from us, including your name, email address, postal address;

(d) information that you provide to us for the purpose of the administration of YFGM, (including but not limited to you making donations; submitting expense claims; submitting bursary applications; and submitting accessibility fund applications), including but not limited to your name, telephone number, email address, and postal address;

(e) any other personal data you choose to share with us.

1.2 Additionally, Young Friends General Meeting may collect, use, and store the following sensitive personal data:

(a) information relating to your religious beliefs, including but not limited to your association with Quaker meetings;

(b) information that you provide to us for the purposes outlined in 1.1.b and 1.1.d, including but not limited to information about your physical or mental health or conditions;

(c) and any other sensitive personal data you choose to share with us.

1.3 Before you disclose to us the personal information of another person, you must obtain that person's consent to both the disclosure and the processing of that personal information in accordance with this policy. You should not share sensitive personal information relating to another person.

2. What will we do with your information?

2.1 Your information will be held by Young Friends General Meeting, which is based at Friends House, 173 Euston Road, London NW1 2BJ and can be contacted at yfgm@quaker.org.uk or 020 7663 1050.

2.2 We will use your information only for the purposes which you have agreed to when providing it, which may include:

(a) running YFGM events;

(b) communicating with you about our work and activities;

(c) processing donations;

(d) processing expense claims;

(e) processing accessibility or bursary applications;

(f) running our Quaker nominations process;

(g) and any other purpose for which you have given consent.

2.3 In most cases, your personal data will be collected and used only on the basis that you have consented to the processing, with the following exceptions:

(a) the processing is necessary to protect your vital interests;

(b) the processing is necessary for compliance with any legal obligation to which Young Friends General Meeting is subject; or

(c) the processing is in accordance with the legitimate interests of Young Friends General Meeting, as set out in legislation.

2.4 In most cases, your sensitive personal data will be collected and used only on the basis that you have explicitly consented to the processing, with the following exceptions:

(a) the processing is necessary to protect your vital interests;

(b) the processing is carried out in the course of YFGM's legitimate activities, as a body which is not established or conducted for profit and exists for religious purposes;

2.5 Young Friends General Meeting of the Religious Society of Friends is the data controller of all personal data that we manage in connection with our work and activities.

2.6 You are not obliged to share your personal data with YFGM. However, failure to do so may prevent YFGM from processing your data in accordance with your wishes. Examples of this may include but are not limited to:

(a) incomplete expenses claims, bursary applications, or accessibility fund applications may not be processed

(b) if you do not provide the information required as part of the registration process for a YFGM event, your registration may not be completed and you may be prevented from attending (see YFGM Constitution 7.4.1)

2.7 The period of time for which your personal data will be stored will be determined by the following criteria:

(a) for a period of three years from the last point at which there is an ongoing relationship between you and YFGM, including but not limited to;

(i) holding an appointed role within YFGM;

(ii) attending a YFGM event;

(iii) making a donation to YFGM;

(iv) opting in to receiving communications from YFGM;

(b) in the case of financial records, for such a period as defined in the relevant policies;

(c) always provided that YFGM shall cease to store your personal data if there is no lawful basis for processing it.

3. Who will have access to your information?

3.1 Young Friends General Meeting of the Religious Society of Friends is the data controller of all personal data that we manage in connection with our work and activities.

3.2 Your data may be shared with data processors, who handle data on behalf of Young Friends General Meeting but do not make decisions on the purposes and means for which any

personal data is processed. In particular, Britain Yearly Meeting of the Religious Society of Friends (BYM) acts as a data processor.

3.3 Your personal data, including where applicable your sensitive data, will be accessible to individuals within YFGM who hold relevant roles, where it is necessary for them to have access to your information to fulfil the relevant purposes. This includes:

(a) the YFGM Coordinator, who is employed by BYM;

(b) the trustees of YFGM;

(c) volunteers with roles within YFGM, including:

(i) the catering coordinator and volunteer caterers;

(ii) members of the Pastoral, Eldership, Nominations, and Logistics Committees;

(iii) in the case of financial information, the YFGM General Fund Treasurer or other members of Finance Committee.

3.4 Any one within YFGM who has access to personal data will be required to be familiar with and uphold YFGM's Data Protection Policy and Privacy Policy.

3.5 YFGM may share your personal data with specific partner organisations to facilitate our charitable purposes or where otherwise necessary. This will only be done on the basis of your explicit consent.

3.6 YFGM may disclose your personal information:

(a) to the extent that we are required to do so by law;

(b) in connection with any ongoing or prospective legal proceedings;

(c) in order to establish, exercise, or defend our legal rights.

3.7 Your data will be stored within the EEA or in countries with an adequate data protection regime, including Guernsey.

4. What do I need to do?

4.1 Young Friends General Meeting will take steps to ensure that all personal data we hold is accurate and up-to-date. To help with this, please let us know if your personal data changes, for example if you move house or change your email address.

4.2 You have the right to withdraw consent for YFGM to hold or process your data. You can withdraw your consent by contacting the YFGM Coordinator.

4.3 You have a range of rights with regard to your personal data. A partial list is included in Section 9.2 of our Data Protection Policy. If you have any queries about these rights, please contact the YFGM Coordinator. These rights include but are not limited to the rights:

(a) to request a copy of any personal data that we hold about you;

(b) to have all personal data erased, unless certain limited conditions apply;

(c) to have inaccurate data amended or destroyed.

5. Security and updates

5.1 We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

5.2 This policy and our Data Protection Policy will be reviewed annually by our board of trustees. We may update this policy from time to time by publishing a new version on our website.