LAST UPDATED: March 2018

DATA PROTECTION POLICY

(FOR INTERNAL USE ONLY)

The Guild of the Royal Hospital of St. Bartholomew

Contents

1. Purpose of the policy

1.1 The Guild of the Royal Hospital of St. Bartholomew (the **"Guild"**) is committed to complying with privacy and data protection laws including:

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

(b) the Privacy and Electronic Communications (EC Directive) Regulations (2003) and any successor or related legislation ("**PECR**"); and

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

(together "**the Legislation**")

1.2 This policy sets out what the Guild does to protect data subjects' personal data.

1.3 Anyone who handles personal data in any way on behalf of the Guild must ensure that they comply with this policy. Section 3 of this policy describes what comes within the definition of "personal data" and sets out the types of personal data that the Guild handles.

1.4 It is important that those carrying out work for the Guild comply with the terms of this policy.

1.5 This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions. The Guild will bring these to your attention on a regular basis where there is a significant change, but it is also your responsibility to check this policy periodically.

2. About this policy

2.1 This policy and any other documents referred to herein sets out the rules on data protection and the legal conditions that must be satisfied when the Guild processes (for example, obtain, handle, store and/or transfer) personal data.

2.2 This policy does not form part of any employee or volunteer contract and may be amended at any time.

2.3 This policy has been approved by the trustees of the Guild.

3. Definitions of key data protection terms and types of personal data processed by the Guild

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

3.2 **Data Subjects** include all living individuals in the EU about whom the Guild holds personal data, for instance a volunteer or a member of the Guild. 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.

Examples of the types of personal data processed by the Guild are as follows:

(a) Full names of data subjects who may be, for example, volunteers/applicants, donors, members and all users of our website/services with whom the Guild communicates;

(b) Contact details, such as postal addresses, telephone numbers and email address;

(c) Financial information, such as credit/debit card details;

(d) Personal descriptions/photographs;

(e) Information about data subjects' computers/mobile devices and their visits to/use of the Guild's website, including for example internet protocol addresses and geographical information; and/or

(f) Any other information shared with us by/collected in relation to data subjects which satisfies the definition of "personal data" per section 3.3.

3.4 **Sensitive Personal Data (which is defined as "special categories of personal data" under the GDPR)** includes information about a data subject'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 condition;

(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.

Sensitive personal data is given additional protection under the Legislation – please see section 14 below. The Guild does not anticipate that it will process sensitive personal data – if you believe that you have been asked to do so, please contact the Chairman and Honorary Secretary (bartsguild@aol.com).

3.5 **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. The Guild is the data controller of all personal data that is processed by the Guild in connection with the Guild's work and activities.

3.6 **Data Processors** are any person who or organisation which 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, for example third party payment processing service providers. Processors also have obligations under the Legislation.

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

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

3.9 **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.

4. Data protection principles

4.1 Anyone processing personal data must comply with the seven data protection principles set out in the GDPR. The Guild is required to comply with these principles (summarised below),

and to be able to prove such compliance (the accountability principle [this is the seventh principle not listed below]), in respect of any personal data that the Guild deals 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, lawfully and transparently

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.

5.1.1 Lawful processing

(a) Processing will only be lawful where the Guild can rely on at least one of the lawful bases provided for in the GDPR for each instance of processing. The Guild is most likely to rely on the following lawful bases:.

(i) The data subject has given their consent to processing (consent must relate to a particular purpose/particular purposes), for example to receive the Guild's newsletter or other promotional material.

(ii) The processing is necessary in order to perform a contract to which the data subject is party, or in order to take steps at the data subject's request prior to entering into a contract, for example where we hire an employee or enter into an agreement with a volunteer.

(iii) The processing is necessary so that the Guild can comply with a legal obligation to which it is subject, for example the administration of its accounts.

(iv) The processing is necessary for purposes of "legitimate interests" pursued by the Guild or a third party. This is a broad term and therefore likely to cover a significant amount of processing carried out by the Guild. In general, processing personal data for the purposes of running the Guild as a charitable entity is likely to be considered a legitimate interest.

However, it should not be selected automatically, nor considered as a last resort. The Legislation requires the Guild to consider, and balance its

legitimate interest against, the concurrent interests, fundamental rights and freedoms of the data subject, as well as their reasonable expectations as to how the Guild will process their personal data based on their relationship with the Guild. For example, this lawful basis may not be available where the processing in question would be excessively intrusive, or where the data subject in question would not reasonably expect the processing in question to take place based on the information given at the time, and context surrounding, the original collection of their personal data. If you have any doubts as to whether this lawful basis is available, or you consider that concurrent interests, fundamental rights and freedoms may prevent the Guild from relying on this lawful basis, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

In particular, the Legislation makes clear that processing children's personal data required careful consideration and additional protection. Therefore, where the data subject is a child (12 and under), please consult the Chairman and Honorary Secretary (bartsguild@aol.com) before proceeding to process that child's personal data using this lawful basis.

(b) There are two further lawful bases available:

(i) Where the processing is necessary to protect the "vital interests" of a data subject or another living individual – for example, where the Guild must process an individual's personal data in an emergency medical situation.

(ii) Where the processing is necessary to perform a task in the public interest – this basis of that performance had to be laid down in UK or EU law.

The Guild does not expect to be able to rely on either of these bases except on rare occasions. If you think that either applies, please consult the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

Please note that in relying on these lawful bases the processing must usually be "necessary" to achieve the relevant purpose. Processing will not be necessary to carry out any of these purposes where the Guild could achieve the purpose in question by other reasonable means, or if the processing is to be carried out only because the Guild operates its business in a particular way. Please consult the Chairman and Honorary Secretary (bartsguild@aol.com) if you have any questions.

We need to justify reliance on a particular lawful basis when we process personal data for a specific purpose. We therefore recommend that you document which lawful basis you are relying on.

(c) In addition, the processing of personal data must not involve a breach of any non-data protection legal provision in UK law. Some common examples include where the processing would involve:

(i) a breach of confidentiality;

(ii) a breach of provisions of a contract; and

(iii) a breach of the Human Rights Act 1998.

5.1.2 Fair processing

In general, the processing carried out by the Guild must also be fair – this is a wide concept so you need to consider the circumstances of the processing in question. For example, processing would be unfair if the Guild collected personal data from a data subject having misled them about why the personal data in question was required.

5.1.3 Transparent processing

In general, the Legislation obliges the Guild to be up front with data subjects about what it does with their personal data and why, and any such information should be communicated to data subjects in a way that is sufficiently straightforward so that a reasonable person would understand.

5.2 One of the most important ways to comply with this principle is that every time the Guild collects personal data about a person directly from that data subject, which the Guild intends to keep, the Guild needs to provide that person with **"** fair processing information**"**. In other words the Guild needs to tell them:

(a) who will be holding their personal data, i.e. The Guild - including contact details and the contact details of our Chairman and Honorary Secretary (bartsguild@aol.com);

(b) why the Guild is collecting their information and what the Guild intends to do with it e.g. to process donations or send mailing updates about our activities;

(c) the legal basis for collecting their information (see section 5(1)(a) above – if the Guild relies on the lawful basis of legitimate interests, those interests must be specified);

(d) 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;

(e) the period for which their personal data will be stored (if it is not possible to give a finite period of time, it is acceptable to provide the criteria which will be used to decide that period – usually the Guild uses criteria related to the purposes for which the personal data is collected/processed);

(f) the existence of the rights of data subjects (please see section 10 below for the rights that must be referred to);

(g) details of people/organisations, or categories of people/organisations, with whom the Guild may share their personal data;

(h) if relevant, the fact that the Guild will be transferring their personal data outside the EEA and details of relevant safeguards (see section 13 below);

(i) The right to lodge a complaint with the Information Commissioner's Office;

(j) The right to withdraw consent if consent is the lawful ground that has been relied upon; and

(k) the existence of any automated decision-making, including behavioural profiling, involving their personal data, including details about the logic involved and the significance and envisaged consequences of such processing for the data subject.

Automated decision-making takes place when personal data is processed solely by automatic means (i.e. where the decision involves no human intervention).

The Guild aims to achieve this by using its Privacy Notice, which is available on its website and made available prior to any data subject providing the Guild with their personal data or, where the personal data is collected from a third party, as soon as reasonably possible thereafter.

5.3 Where the Guild obtains personal data about a data subject from a source other than the data subject, the Guild must still provide that individual with its Privacy Notice that sets out the information listed in section 5.2 above (apart from the requirement in section 5.2 (d)) as well as information on:

(a) the categories of personal data and

(b) information on the source of the personal data, and whether this is a publicly available source.

There are limited exceptions from the requirement to provide a Privacy Notice in such circumstances.

5.4 This fair processing information, as contained in the Guild's Privacy Notice, can be provided in a number of places including on web pages, in mailings or on application forms. The Guild 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 determined by the Guild when the Guild first obtained the personal data, or for a compatible purpose.

6.2 This means that the Guild should not collect personal data for one purpose and then use it for another incompatible purpose. If it becomes necessary to process a data subject's personal data for a new purpose, the individual should be informed of the new purpose beforehand. For example, if the Guild collects personal data such as a contact number or email address, in order to update a data subject 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 limited to what is necessary

In effect, the third data protection principle requires that personal data processed by the Guild should be limited to what is necessary in relation to the purposes for which it is processed.

This means that, considering the purposes specified in the Guild's Privacy Notice available online, the Guild can only collect the amount/type of personal data that is strictly necessary to achieve the purpose(s) in question.

8. Personal data should be accurate and where necessary kept up to date

The Guild is obliged to take reasonable steps to ensure that inaccurate personal data is corrected and that out of date personal data is updated – our Privacy Notice sets out means for data subjects to do this, but if you are aware that any personal data processed by the Guild is inaccurate and/or out of date, please take steps to amend it accordingly and record those steps and the fact that the personal data has been amended.

9. Not retaining personal data for longer than necessary

9.1 The fifth data protection principle requires the Guild to not keep personal data for longer than required for the purpose it was collected. This means that the personal data that the Guild holds should be destroyed or erased from our systems when it is no longer needed. If you think that the Guild is holding out-of-date personal data, please speak to the Chairman and Honorary Secretary (bartsguild@aol.com).

9.2 In general, the Guild will keep personal data for 6 years from the time it is collected or 6 years after the last interaction with the individual, unless:

9.2.1 the purpose for which the Guild collected the personal data in question has been fulfilled, and there is no other purpose to carry on processing it;

9.2.2 the lawful basis for which is it processed has expired (for example, where processing is based on a data subject's consent and that consent has been withdrawn); or

9.2.3 Where the purpose for processing it, and underlying lawful basis, remains valid after 6 years.

10. Rights of individuals under the GDPR

10.1 The GDPR gives data subjects specific rights in relation to how organisations process their personal data which they can exercise by contacting the Guild. Everyone who processes personal data on behalf of the Guild needs to be aware of these rights. These rights are listed below:

10.2 <u>Right of Access</u>

A data subject has the right:

(a) To obtain confirmation of whether the Guild is processing his or her personal data;

(b) to request a copy of any personal data that the Guild holds about them (as data controller); and

(c) where the Guild is processing their personal data, to access the following information:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) to the extent not already provided to the data subject (by way of the Guild's Privacy Notice), the categories of information specified in section 5.2(b); (e); (g) and (k) above and the categories and the existence of the rights as outlined in section 10.3; 10.4; 10.5; 10.7 and 10.8 below;

(iv) if any recipients of their data are an international organisation or based in a Third Country (see definition in section 14.3 below) and, if so, what appropriate safeguards the Guild has adopted to ensure that their personal data is adequately protected (see section 14 below);

(v) the categories of personal data concerned; and

(vi) where the personal data was not collected from the data subject, any information available as to its source.

Please keep a record of when a request to exercise the right of access has been made. The Legislation obliges the Guild to provide the requested information without delay and, at the latest, within one month of receipt. The Guild can extend the period of compliance by a further 2 months where requests are complex or numerous – if you are ensure whether the Guild can use this extension, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

The Guild may either charge a reasonable fee or refuse to respond where requests are manifestly unfounded or excessive. If you consider that this may be the case, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

In general, the Guild's policy is to provide the requested information by email.

10.3 Right to rectification

A data subject has the right to have inaccurate or incomplete personal data amended.

Where the Guild has disclosed inaccurate or incomplete data to a third party, the Guild is obliged to inform that third party where appropriate. If you receive a request to rectify personal data, please therefore check whether the inaccurate/incomplete personal data in question has been disclosed to any third parties.

Please keep a note of when the request to exercise the right of rectification has been made – the Guild is obliged by the Legislation to reply within one month. This period can be extended by two months where the request is complex – if you consider this to be the case, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

10.4 Right to erasure (also known as the right to be forgotten)

A data subject has the right to request that all of his or her personal data is deleted or removed from the Guild's records where there is no compelling reason for its continued processing. The right is only available in specific circumstances:

(a) Where it is no longer necessary for the Guild to process the personal data in relation to the purpose for which it was originally collected/processed.

(b) Where the only lawful basis for processing the personal data was the data subject's consent and the data subject withdraws that consent (see section 10.10 below).

(c) When the data subject objects to the processing and there is no overriding legitimate interest for continuing the processing (see section 10.7 below).

(d) The personal data was unlawfully processed (see section 5.1(b) above).

(e) Where the personal data has to be erased in order to comply with a legal obligation (if you receive such a request, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

(f) Where the personal data is processed in relation to the offer of information society services ("**ISS**") to a child (12 and under). An ISS is any online service.

If the above categories involve processing that causes unwarranted and substantial damage or distress to the data subject, this will likely make the case for erasure stronger.

However, even when those circumstances apply, there are exceptions which can allow the Guild to refuse to comply with a request for erasure. These exceptions apply where the personal data in question is processed:

(a) So that the Guild can exercise the right of freedom of expression and information.

(b) So that the Guild can comply with a legal obligation for the performance of a task in the public interest or in the exercise of official authority.

(c) For public health purposes in the public interest.

(d) For archiving purposes in the public interest; scientific or historical research or statistical purposes; or

(e) The exercise or defence of legal claims

Please see section 5(1)(a)(v) above in relation to the notion of the public interest.

Where the Guild has disclosed to a third party personal data which must be erased, the Guild is obliged to inform the third party about the erasure, unless it is impossible or involves disproportionate effort to do so (please contact the Chairman and Honorary Secretary (bartsguild@aol.com) if you consider this to be the case). Where those third parties operate online and have made personal data public, the Guild should ask such third parties to erase links to, copies or replications of the personal data. Please therefore consider whether the Guild has disclosed the personal data in question to a third party. If you receive a request for erasure, and consider that the Guild must comply, please therefore check whether personal data in question has been disclosed to any third parties.

10.5 Right to restrict processing

Data subjects have the right to block/suppress processing of personal data in certain circumstances. When the right is exercised, the Guild can continue to store the personal data, but engage in no other form of processing. The Guild can store only enough personal data about the data subject such that the restriction can be respected in the future.

The right only applies in the following circumstances:

(a) Where a data subject contests the accuracy of personal data, you should restrict any further processing operations in relation to that personal data until you/the Guild has verified its accuracy.

(b) Where an individual has objected to the processing (see section 10.7 below) and the Guild is considering whether it has legitimate grounds to refuse the request.

(c) When the processing in question is unlawful but the data subject prefers restriction as the solution instead of erasure.

(d) Where the Guild no longer requires the personal data, but the data subject requires the data to establish, exercise or defend a legal claim.

Where the Guild has disclosed the personal data in question to a third party, the Guild is obliged to inform them about the restriction on the processing of personal data, unless to do so is impossible or involves disproportionate effort. Please therefore consider whether the Guild has disclosed the personal data in question to a third party.

10.6 Right to data portability

Data subjects are entitled to obtain and reuse their personal data across different services. This right therefore allows them to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, and without hindrance to usability.

The right only applies where:

(a) the data subject in question has provided the personal data in question to the Guild;

(b) where the lawful basis for processing is either the data subject's consent or for the performance of a contract (see sections 5(1)(a)(i) and (ii) above); and

(c) where the processing in question is carried out by automated means (see section 5.2(k) above).

Where the right applies, the Guild must provide the personal data in a structured, commonly used and "machine-readable" form. In this context, machine-readable means that the personal data is structured so that software can extract specific elements of the personal data (so as to enable other organisations to use it). Please ask Chairman and Honorary Secretary (bartsguild@aol.com) if you are unsure how to comply with this right.

The Guild must respond to such a request without undue delay, and at the latest within one month. The Guild can extend the period for compliance by two months where the request is complex or numerous – however, the data subject must be informed within one month of receipt that the Guild considers the extension necessary, with reasons. Please therefore keep a record of the date the request to exercise this right was made.

If you do not consider that the Guild is obliged to respond, or you are not sure, please contact the Chairman and Honorary Secretary (bartsguild@aol.com). The Guild must explain why it is not responding to the data subject, informing them of their right to complain to the ICO (see section 10.9 below) and to a judicial remedy. This explanation must be provided without undue delay, and at the latest within one month.

10.7 Right to object

A data subject has the right to object to the processing of their personal data in three different circumstances. These are where:

(a) processing of their personal data where that processing is based on the lawful bases of the Guild's legitimate interests or public interests (see sections 5(1)(a)(v) and (vi) above);

The Guild must stop processing their personal data unless:

(i) the Guild can demonstrate compelling legitimate grounds for continuing the processing, which override the interests, rights and freedoms of the data subject; or

(ii) the processing is for the establishment, exercise or defence of legal claims.

Please note that, where the Guild processes their personal data on either of these lawful bases, the Guild is obliged under the Legislation to inform data subjects of their right to object at the Guild's first point of communication with them, **in addition to** informing them via the Guild's Privacy Notice. The right must be explicitly brought to data subjects' attention and must be presented clearly and separately from any other information contained in that first communication – for example, where the communication is by email, please include information as to this right in a separate paragraph using bold or underlined script. Where processing is based on either of these 2 lawful bases and you plan to communicate with the data subject, please therefore check whether this is the first communication from the Guild to them.

(b) Processing of their personal data for purposes of direct marketing (including "behavioural profiling" – in this context, behavioural profiling means collecting information about a data subject – for example about their personal interests or the Guild's opportunities which have interested them – in order to inform the Guild's advertising strategy).

As soon as the Guild receives an objection, processing for the purposes of direct marketing must stop – there are no exemptions or grounds to refuse to comply.

Where processing is for direct marketing purposes, individuals must be informed of their right to object at the first point of communication and in the Guild's privacy notice.

(c) Processing of their personal data for the purposes of scientific or historical research and statistics.

To exercise this right, data subjects must show that their objection is based on grounds relating to his or her particular situation. If they can do this, then the Guild must stop the processing in question, unless it is conducting research where the processing of personal data is necessary for the performance of a task in the public interest, in which case the

Guild may continue the research in question. Please see section 5(1)(a)(v) for an explanation as to the notion of the public interest.

10.8 Rights related to automated decision making (including profiling):

As discussed in sections 5.2(k) and 10.7(b) above, the GDPR contains provisions which apply to:

(a) automated decision-making (making a decision solely by automated means without any human involvement); and

(b) profiling (automated processing of personal data to evaluate certain things about a data subject, for example their individual preferences and interests).

Where processing only involves automated decision-making that has legal or similarly significant effects on them, the Guild can only carry out such decision-making where the decision is:

(a) necessary for the entry into or performance of a contract (i.e. which does not necessarily need to involve the Guild and/or the data subject); or

(b) authorised by EU or UK law – please contact [insert name of person with authority for data protection matters]; or

(c) based on the data subject's explicit consent.

Where the Guild undertakes automated decision-making, the Guild must:

(a) give data subjects information about the processing;

(b) introduce simple ways for data subjects to request human intervention or challenge a decision; and

(c) carry out regular checks to make sure that the Guild's systems are working as intended. To the extent that you will be involved in such checks, you will be given information/training at the appropriate time.

10.9 Right to lodge a complaint with the ICO

Data subjects have a general right to lodge a complaint with the ICO about any aspect of the Guild's processing of their personal data. The Guild informs data subjects of this right by providing the ICO's contact details in its Privacy Notice – any communications we receive from the ICO should be directed to the Chairman and Honorary Secretary (bartsguild@aol.com). If you receive any such communication, please contact, and ensure it is directed to, the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

10.10 Right to withdraw consent

Where the Guild's processing activities are based solely on a data subject's consent – for example, in relation to direct marketing – the data subject has the right to withdraw their consent at any time. The Guild informs data subjects of this right in its Privacy Notice and

whenever it collects consent for relevant processing activities. If you are obtaining a data subject's consent to any data processing activity, please make sure that they are expressly informed about their right to withdraw that consent at any time. If you have any cause to believe that a data subject has not been adequately informed about their right to withdraw consent, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) immediately.

10.11 Where requests to exercise data subjects' rights are received

Requests from data subjects to exercise these rights may be received by email, telephone or written post. Data subjects are instructed by the Guild's Privacy Notice to direct their requests to the Chairman and Honorary Secretary (bartsguild@aol.com), but should any such request come straight to you, or should you have any doubt as to whether a request to exercise a right has been made, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) immediately.

11. Data security

11.1 The sixth data protection principle requires that the Guild keep secure any personal data that the Guild holds.

11.2 The Guild is required to put in place "organisational" and "technical" procedures to keep the personal data that the Guild holds secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In general, organisational measures include measures such as internal training on how to recognise personal data and where it should be stored/what can and cannot be done with it, while technical measures include IT measures such as security of wireless internet networks and anti-virus software. The Guild is responsible for devising, developing and implementing such measures and will train/inform you about such measures at the appropriate time.

11.3 When you deal with sensitive personal data, more rigorous security measures are likely to be needed, for example if sensitive personal data is held on a memory stick or other portable device it should always be encrypted. You will receive training/information at the appropriate time.

11.4 When deciding what level of security is appropriate, please first consult the Guild's Privacy Policy, available online. Your starting point should be to look at whether the personal data is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands. If you have any doubts, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

11.5 The Guild has implemented the following security procedures and monitoring processes that must be followed in relation to all personal data you process on behalf of the Guild:

(a) measures to restore availability and access to data in a timely manner in event of physical or technical incident;

(b) process for regularly testing, assessing and evaluating effectiveness of security measures;

(c) regular back-ups should be taken of all data on the system and storing data on local drives or removable media should be avoided where possible, as these will not be backed up;

(d) staff/volunteers should ensure that individual monitors do not show confidential information or sensitive personal data to passers-by and that they log off from their PC when it is left unattended;

(e) 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;

(f) 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);

(g) other measures to ensure confidentiality, integrity, availability and resilience of processing systems;

(h) desks and cupboards should be kept locked if they hold confidential or sensitive personal data;

(i) staff must keep data secure when travelling or using it outside the offices; and

(j) the Guild operates a system of data anonymisation when processing personal data to collect statistics on the activities facilitated by its website. The types of personal data which will be anonymised include information about donors, members and subscriptions, details of online sales and grant applications.

12. Travelling with personal data and remote working

12.1 Staff/volunteers must keep personal data secure while travelling or using it outside our offices. For instance:

(a) documents and laptops must be kept secure (not left lying around off site);

(b) when using any device that enables encryption – for example USB sticks or portable hard drives, data should be encrypted;

(c) mobile devices should be equipped with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft; data stored on computers when working at home must be password protected, and kept confidential;

(d) 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;

(e) any paper documents or files containing confidential and/or sensitive personal data should be kept in lockable desks or filing cabinets; and

(f) Where any document or electronic device contains sensitive personal data, it should never be left open to be viewed by anybody except the staff

member/volunteer handling it, and should be locked by password access or kept in a lockable cabinet or drawer.

13. Transferring Data Outside the EEA

13.1 The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected.

13.2 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, but this list may be updated.

13.3 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 included in the list in section 13.2 or the USA (see section 13.4 below) ("Third Countries"), it will be necessary to enter into an EC-approved agreement (e.g. the Standard Contractual Clauses), seek the explicit consent of the data subject, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA. If you know or become aware that personal data will be transferred to a Third Country, please speak to the Chairman and Honorary Secretary (bartsguild@aol.com) before carrying out any such transfer.

13.4 The EU-US Privacy Shield (the "Shield") is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, but only if such an organisation is a signatory to the Shield. Specific advice should be sought from the Chairman and Honorary Secretary (bartsguild@aol.com) before transferring personal data to organisations in the US.

13.5 Please note that this section may need to be revised depending on the outcome of the UK's negotiation with the EU as part of the Brexit process.

13.6 For more information, please speak to the Chairman and Honorary Secretary (bartsguild@aol.com).

14. Processing sensitive personal data

14.1 On some occasions the Guild may collect information about individuals that is defined by the GDPR as **special categories of personal data**, and special rules will apply to the processing of this data. This policy refers to "special categories of personal data" as "sensitive personal data". The categories of sensitive personal data are set out in the definition in Section 3.4.

14.2 Financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously. Data about criminal offences is also subject to stricter rules.

14.3 In order to process sensitive personal data, the Guild must meet one condition from a list of additional conditions to be able to process that sensitive personal data lawfully. The conditions likely to be relevant to the Guild's work and services are:

(a) explicit consent of the data subject;

(b) processing in compliance with employment law obligations;

(c) vital interests of the data subject;

(d) processing carried out in the legitimate interests of a not-for-profit organisation;

(e) information made public by the data subject; and

(f) legal advice and establishing/defending legal rights.

Please note that (i) depending on the circumstances, there may be other conditions available and (ii) the conditions are only available in limited circumstances. If you have any doubts as to the availability of the conditions, or whether/how a condition can be relied on, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

15. Entering into contracts with data processors

15.1 The Guild uses data processors (see definition in section 3.6 above) to carry out certain data processing activities on its behalf – for example, the administration of donations and membership payments is handled by a third party service provider.

15.2 Where the Guild engages data processors, there are a number of obligations it must comply with:

(a) Where the activities undertaken pursuant to a data processing contract involve transferring personal data outside of the EEA, please refer to section 13 above.

(b) The Guild may only use data processors who offer sufficient guarantees to meet the requirements of the Legislation and protect data subjects' rights. In general, where you are instructed to perform a task in relation to a data processing agreement by a senior member of staff, you may assume that the Guild is satisfied that the data processor in question has provided sufficient guarantees. However, if you have any reason to doubt:

(i) that sufficient guarantees have been given; and/or

(ii) that the data processor in question is complying with its obligations under the data processing agreement or Legislation; and/or

(iii) that the person instructing you is senior enough to know with certainty that the Guild is satisfied that data processor has offered sufficient guarantees;

please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

(c) The Guild must enter into a written agreement with the data processor which sets out (i) the subject matter, duration, nature and purpose(s) of the processing; (ii) the type(s) of personal data and (iii) the categories of data subjects which will be processed.

In relation to the data processor, the data processing agreement must provide:

(i) that the data processor will not engage another data processor without the prior specific or general written authorisation of the Guild;

(ii) that the data processor will only process personal data based on documented instructions from the Guild;

(iii) that the person(s) authorised to process the personal data on the Guild's behalf commit to the confidentiality of the personal data;

(iv) that the data processor will take organisational and technical security measures appropriate to the nature, scope, context and purposes of processing, the type(s) of personal data involved and the associated risks to data subjects;

(v) that the data processor will facilitate the Guild's obligations to comply with data subjects' request to exercise their rights as detailed in section 10;

(vi) that, bearing in mind the nature of the processing and information available to the data processor, the data processor will assist the Guild in complying with the following obligations:

(A) the Guild's security obligations as set out in section 11 above;

(B) the Guild's obligation to report security breaches as set out in section 16 below – in particular, the data processor must notify the Guild without undue delay after becoming aware of a security breach and, where appropriate, must provide information as to the nature of the breach, the categories and approximate numbers of data subjects involved and the measures taken to mitigate potential adverse effects; and

(C) where appropriate, conducting a data protection impact assessment ("DPIA") and/or consulting with the ICO prior to commencing processing likely to result in a high-risk to the rights and freedoms of natural persons. To the extent that the Guild conducts a DPIA and/or consults with the ICO and you become involved, you will receive appropriate training and information at the relevant time;

(vii) that the data processor is obliged, at the choice of the Guild, to delete or return all the personal data concerned to the Guild at the end of the provision of data processing services; and

(viii) makes available to the Guild all information necessary to demonstrate compliance with obligations under the Legislation.

15.3 In general, if you have any reason to believe that the Guild and/or the relevant data processor is not complying with its obligations, or that the underlying DPA does not comply with the Legislation, please contact the Chairman and Honorary Secretary (bartsguild@aol.com) in the first instance.

16. The role of the Information Commissioner's Office

16.1 There is no obligation for the Guild to make an annual notification to the ICO under the GDPR, but the Guild may consult with the ICO where necessary when the Guild carrying out "high risk" processing. You may be involved in any such consultation. Additionally, there may be a requirement to pay an annual fee to the ICO.

16.2 The Guild must report data security breaches (other than those which are unlikely to be a risk to individuals) to the ICO where feasible, and within 72 hours of becoming aware of the data security breach. A data security breach may have occurred where personal data has been compromised in some way (for example through sending it outside the control of the Guild, or misplacing a laptop in a public place which contains personal data – please see section 12 above).

16.3 The Guild is required to notify affected data subjects where a data security breach is likely to result in a high risk to the rights and freedoms of these data subjects. The obligation to notify may not be required in certain circumstances where the personal data is encrypted or the Guild has taken subsequent measures to ensure that the high risk to data subjects is not likely to materialise.

16.4 If you are unsure whether a data security breach has occurred or, in any case, if you think data breach has occurred, please immediately notify the Chairman and Honorary Secretary (bartsguild@aol.com).

17. Monitoring and review of the policy

This policy is reviewed annually by our board of trustees to ensure that it is achieving its objectives. The Guild may otherwise update it from time to time so please check it periodically.