Data Protection Procedures and Guidance Note

Data Protection Procedures and Guidance Note

1. Introduction

1.1 The aim of this note is to ensure that Making Me (the **Charity**) and its trustees, contractors and employees (including volunteers) are informed about their obligations under the General Data Protection Regulation (the **GDPR**), the Data Protection Act 2018 and any other relevant data protection legislation, and are thus able to comply with those obligations and the requirements of the Charity's Data Protection Policy and Privacy Policy. References in this guidance note to the GDPR include, where appropriate, the Data Protection Act 2018 and that other legislation.

1.2 The Charity recognises its responsibility to hold all personal data securely and use it only for legitimate purposes with the knowledge and approval of the data subjects, in a manner which is proportionate to the nature of the personal data being held by the Charity. This note and the related policies are based on the trustees' assessment in good faith of the potential impacts on both the Charity and its data subjects of the personal data being stolen, abused, corrupted or lost.

1.3 This note applies to all staff, including voluntary staff and should be read in conjunction with the Data Protection Policy, the Privacy Policy and the Charity's other policies, including, but not limited to the Safeguarding and Child Protection Policy.

1.4 This note will be monitored periodically in order to judge its effectiveness and reviewed annually. It will be updated as required in accordance with changes in the law.

2. Definitions

The following definitions apply for terms used in this note:

2.1. *Consent of the Data Subject* means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

2.2. *Data* is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

2.3. *Data Controller* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

2.4. *Data Processor* means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

2.5. *Data Subject* means an identifiable living individual 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;

2.6. *Data Users* include contractors, employees, volunteers and trustees whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

2.7. *FOIA* means the Freedom of Information Act 2000;

2.8. *ICO* means the Information Commissioner's Office;

2.9. *Parent* has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

2.10. *Personal Data* means any information relating to an identified or identifiable Data Subject; and an identifiable Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

2.11. *Personal Data Breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

2.12. *Processing* means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. General

3.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat that information in an appropriate and lawful manner.

3.2 The type of information that we may be required to handle includes (but is not limited to) details of job applicants, current, past and prospective clients/service users, donors, contractors, employees, pupils, trustees, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

4. Status of the policy and guidance note

4.1 The Data Protection Policy, the Privacy Policy and this guidance note have been approved by the Trustees of the Charity. They set out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

4.2 The Data Protection Policy, the Privacy Policy and this guidance note do not form part of any client's or contractor's terms of engagement or employee's contract of employment, and they may be amended at any time. Any failure by a member of staff to comply will be taken seriously and may result in disciplinary action; serious breaches may result in dismissal. Breach of the GDPR may expose the Charity to enforcement action by the ICO, including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Charity's members or other staff. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the Charity and for our stakeholders.

5. Data Controller and Data Protection Officer / responsible person

5.1 The Making Me charity is the Data Controller for all the Personal Data processed by the Charity.

5.2 In the opinion of the Trustees, having referred to the checklist and tool on the ICO website, as at the date of the Data Protection Policy and this guidance note, the scope and nature of the Personal Data held by the Charity is not sufficient to warrant the appointment of a Data Protection Officer.

5.3 The Chief Executive of the Charity is responsible for ensuring the Charity is compliant with the GDPR and with the Charity's Data Protection Policy and Privacy Policy. This post is held by Elizabeth Fordham. The Chief Executive will report directly to the Trustees.

5.4 If any member of staff or volunteer considers that the Charity's Data Protection Policy, the Privacy Policy or this guidance note has not been followed in respect of Personal Data about themselves or others, they should raise the matter with the Chief Executive.

6. Data protection principles

Anyone processing Personal Data must comply with the principles of Article 5 of the GDPR, as set out in paragraph 2 of the Charity's Data Protection Policy.

7. Processing

7.1 The GDPR is intended not 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. The Data Subject must be told who the Data Controller is (in this case the Charity), who the Data Controller's representative is, the purpose for which the data is to be Processed, and the identities of anyone to whom the Data may be disclosed or transferred.

7.2 For Personal Data to be processed lawfully, certain conditions have to be met. These include:

7.2.1 where we have the Consent of the Data Subject – see paragraph 10 below;

7.2.2 where a contract between the Data Subject and the Charity permits this;

7.2.3 where it is necessary for compliance with a legal obligation, e.g. in order to manage an employee's taxation affairs, information may need to be collected, processed and shared with HMRC;

7.2.4 where processing is necessary to protect the vital interests of the Data Subject or another person;

7.2.5 where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and

7.2.6 where it is in the legitimate interests of the Charity to hold such Personal Data on its trustees, staff, volunteers, clients and donors as will enable it to communicate efficiently and effectively with them on matters relating to the operation of the Charity.

7.3 Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected (see paragraph 9 below), or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

8. Sensitive Personal Data and Confidential Information

8.1 The Charity will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

8.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 7.2 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

8.2.1 the Data Subject's explicit Consent to the processing of such Data has been obtained;

8.2.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

8.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent; or

8.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

8.3 The Charity recognises that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

9. Transparency and privacy notices

9.1 One of the key requirements of the GDPR relates to transparency. This means that the Charity must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

9.2 One of the ways we provide this information to individuals is through a privacy communication which sets out important information about what we do with their Personal Data. See the Charity's separate Privacy Policy.

9.3 The Charity wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy policy is just one of the tools we will use to communicate this information. Contractors and employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our Privacy Policy and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to Charity premises or if we ask people to complete forms requiring them to provide their Personal Data.

9.4 We will ensure that privacy communications are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

10. Consent

10.1 The Charity must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent – see paragraph 7.2 above.

10.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

10.3 If we are relying on Consent as a basis for Processing Personal Data about pupils, and a pupil is aged under 13, we will need to obtain Consent from the Parent(s). If we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, depending on the circumstances, the Charity should consider whether it is appropriate to inform Parents about this process.

10.4 Consent is also required if, for example, the Charity wishes to use a photo of a pupil on its website or on social media, and before any pupils are signed up to online learning platforms. Such Consent must be from the Parent is the pupil is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

10.5 Data Subjects must be easily able to withdraw Consent to Processing at any time, and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a purpose which was not disclosed when the Data Subject first consented.

10.6 Unless we can rely on another legal basis of Processing, explicit Consent is usually required for Processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require explicit Consent) to Process most types of Sensitive Personal Data.

10.7 Evidence and records of Consent must be maintained so that the Charity can demonstrate compliance with Consent requirements.

10.8 See also the checklists for consents and other related information on the ICO website at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

11. Purposes of collection and processing

11.1 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, at the point of collecting the Personal Data. Any Personal Data which is not necessary for that purpose should not be collected in the first place.

11.2 The Charity will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

12. Adequacy and relevance of Personal Data

12.1 The Charity will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

12.2 In order to ensure compliance with this principle, the Charity will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

12.3 Staff must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate the Charity's function and we should not collect excessive Personal Data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

12.4 The Charity will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff or trustees who need to know Personal Data about a Data Subject will be given access to it, and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the Charity may adopt a layered approach in some circumstances, for example, members of staff or trustees may be given access to basic information about a pupil, contractor or employee if they need to know it for a particular purpose, but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

13. Accuracy of Personal Data

13.1 Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Personal Data should be destroyed.

13.2 If a Data Subject informs the Charity of a change of circumstances their records will be updated as soon as is practicable.

13.3 Where a Data Subject challenges the accuracy of their Personal Data, the Charity will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Chief Executive for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the ICO. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

13.4 Notwithstanding paragraph 13.3, a Data Subject continues to have rights under the GDPR and may refer a complaint to the ICO regardless of whether the procedure set out in paragraph 13.3 has been followed.

14. Duration of Personal Data storage

14.1 Personal Data should not be kept longer than is necessary for the purpose for which it is held. This means that Personal Data should be destroyed or erased from our systems when it is no longer required.

14.2 It is the duty of the Chief Executive, after taking appropriate guidance for legal considerations, to ensure that obsolete Personal Data are properly erased.

15. Security of the Personal Data

15.1 The Charity has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

15.2 The GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

15.3 We will develop, implement and maintain safeguards (including use of encryption and pseudonymisation where applicable) which are appropriate to our size, our available resources, the amount of Personal Data that we own or maintain on behalf of

others, and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

15.4 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

15.5 It is the responsibility of all members of staff and trustees to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Chief Executive.

16. Data Subjects' rights

16.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

16.1.1 withdraw Consent to Processing at any time;

16.1.2 receive certain information about the Data Controller's Processing activities;

16.1.3 request access to their Personal Data that we hold;

16.1.4 prevent our use of their Personal Data for direct marketing purposes;

16.1.5 ask us to erase Personal Data if it is no longer needed in relation to the purposes for which it was collected or Processed, or to rectify inaccurate or incomplete Data;

16.1.6 restrict Processing in specific circumstances;

16.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

16.1.8 object to decisions based solely on automated processing, including profiling (Automated Decision Making);

16.1.9 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

16.1.10 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

16.1.11 make a complaint to the supervisory authority (the ICO); and

16.1.12 in limited circumstances, ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

16.2 Members of staff should not allow third parties to persuade them to disclose Personal Data without proper authorisation, and should be required to verify the identity of an individual requesting Data under any of the rights listed above.

17. Subject Access Requests

17.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them (a "Subject Access Request") must be made in writing. The Charity can invite a Data Subject to complete a request form but we may not insist that they do so.

17.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request, or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the Charity from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the FOIA. Requests for information under the FOIA must be dealt with promptly and in any event within 20 working days.

17.3 Any member of staff who receives a written request of this nature must immediately forward it to the Chief Executive as the statutory time limit for responding is one calendar month.

17.4 A fee may not be charged to the individual for provision of this information.

17.5 The Charity may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

17.6 Requests from children who are considered mature enough to understand their rights under the GDPR will be processed as a Subject Access Request as outlined below, and the data will be given directly to the child (subject to any exemptions that apply under the GDPR or other legislation). As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights. In every case it will be for the Charity, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

17.7 Requests from children who do not appear to understand the nature of the request will be referred to their Parent.

17.8 Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the Charity considers the child to be mature enough to understand their rights under the GDPR, the Charity shall ask the child for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the Charity to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the Charity shall not disclose the Personal Data if to do so would breach any of the data protection principles.

17.9 Following receipt of a Subject Access Request, and provided that there is sufficient information to process the request, an entry should be made in the Charity's Subject Access records, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required, and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the record will be the date on which sufficient information has been provided.

17.10 Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the Charity can:

17.10.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

17.10.2 refuse to respond.

17.11 Where we refuse to respond to a Subject Access Request, the response must set out the reasons why to the individual, informing them of their right to complain to the supervisory authority and to pursue a judicial remedy, without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the Chief Executive before refusing a request.

17.12 Certain information may be exempt from disclosure, so members of staff will need to consider what exemptions (if any) apply and decide whether the Charity can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely, or that you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the Chief Executive if you are unsure which exemptions apply.

17.13 A Subject Access Request is normally part of a broader complaint or concern, or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request. See also the Charity's separate Complaints Policy.

18. Providing information over the telephone

18.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the Charity whilst also applying common sense to the particular circumstances. In particular, they should:

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

18.1.2 suggest that the caller put their request in writing if they are not sure about the caller's identity or where their identity cannot be checked; and

18.1.3 refer to their line manager or the Chief Executive for assistance in difficult situations. No- one should feel pressurised into disclosing personal information.

19. Authorised disclosures

19.1 The Charity will only disclose Data about individuals if one of the lawful bases apply.

19.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The Charity will regularly share Personal Data with third parties where it is lawful and appropriate to do so.

19.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right, in which case we will be joint controllers of Personal Data and may be jointly liable in the event of any data breaches.

19.4 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances, but a record of the decision and the reasons for sharing information should be kept.

19.5 All Data Sharing Agreements must be signed off by the Chief Executive, who will keep a register of all Data Sharing Agreements.

19.6 The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is

Processed ("GDPR clauses"). It will be the responsibility of the Charity to ensure that the GDPR clauses have been added to the contract with the Data Processor. Personal Data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

20. Reporting a Personal Data Breach

20.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

20.2 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to the individuals.

20.3 If the breach is likely to result in high risk to affected Data Subjects, the GDPR requires organisations to inform the ICO without undue delay.

20.4 It is the responsibility of the Chief Executive, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

20.5 As the Charity is closed or has limited staff available during holiday periods there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected.

21. Accountability

21.1 The Charity must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

21.2 The Charity must have adequate resources and controls in place to ensure and to document GDPR compliance including:

21.2.1 providing appropriate training for employees and trustees on the GDPR, this guidance note, the Data Protection Policy, the Privacy Policy, related policies and data protection matters including, for example, Data Subjects' rights, Consent, legal bases and Personal Data Breaches. The Charity must maintain a record of training attendance by Charity personnel; and

21.2.2 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

22. Record keeping

22.1 The GDPR requires us to keep full and accurate records of all our Data Processing activities.

22.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

22.3 These records should include, at a minimum, the name and contact details of the Data Controller and the Chief Executive, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

23. Review

23.1 It is the responsibility of the Trustees to facilitate the review of this guidance note, the Data Protection Policy and the Privacy Policy on a regular basis. Recommendations for any amendments should be reported to the Chief Executive.

23.2 We will continue to review the effectiveness of this guidance note, the Data Protection Policy and the Privacy Policy to ensure they are achieving their stated objectives.

24. Enquiries

24.1 Questions about the Charity's Data Protection Policy or this guidance note should be directed to the Chief Executive.

24.2 General information about the GDPR can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Signed: Name:

Position:

Date:

Date of next Review: