Data Protections

1. INTRODUCTION

1.1. Ageing Better, "the Charity" is the Data Controller for the purposes of the EU General Data Protection Regulation.

1.2. The Charity collects and uses certain types of personal information about the following categories of individuals:

1.2.1. Staff;

1.2.2. Volunteers including Trustees;

1.2.3. Beneficiaries;

1.2.4. Donors;

and other individuals who come into contact with Ageing Better.

1.3. The Charity will process this personal information in the following ways:

1.3.1. Storing

1.3.2. Financial transactions

1.3.3. Compliance with legsliation

1.3.4. to comply with statutory and contractual obligations relating to employment;

1.3.5. to comply with statutory and other legal obligations relating to safeguarding.

1.4. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the EU General Data Protection Regulation (the "GDPR") and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

1.5. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.6. This policy will be updated as necessary to reflect best practice, or amendments made to the GDPR, and shall be reviewed every 2 years.

2. PERSONAL DATA

2.1. 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.1.1. race or ethnic origin;

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

2.1.6. an individual's sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3. THE DATA PROTECTION PRINCIPLES

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, the Charity is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3. The Charity is committed to complying with the principles in 3.1 at all times. This means that the Charity will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Records Retention Policy;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

4. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

4.1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given;

4.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request;

4.3. The processing is necessary for the performance of a legal obligation to which we are subject;

4.4. The processing is necessary to protect the vital interests of the individual or another;

4.5. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us;

4.6. The processing is necessary for a legitimate interest of the Charity or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned. More details of this are given in the Privacy Notice [or state where this information can be found if relevant].

5. DISCLOSURE OF PERSONAL DATA

5.1. The following list includes the most usual reasons that the Charity will authorise disclosure of personal data to a third party:

5.1.1. to give a confidential reference relating to a current or former employee, [or volunteer];

5.1.2. for the prevention or detection of crime;

5.1.3. for the assessment of any tax or duty;

5.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract) [if you know of any such obligations e.g. under Freedom of Information legislation, duties to the LA etc. please list them as specifically as you can];

5.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

5.1.6. for the purpose of obtaining legal advice;

5.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

5.2. The Charity may receive requests from third parties (i.e. those other than the data subject, the Charity, and its employees) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the

GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or the Charity.

5.3. All requests for the disclosure of personal data must be sent to the Director of Operations and Finance, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

6. SECURITY OF PERSONAL DATA

6.1. The Charity will take reasonable steps to ensure that members of staff [and volunteers] will only have access to personal data where it is necessary for them to carry out their duties. All staff [and volunteers] will be made aware of this Policy and their duties under the GDPR. The Charity will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.2. For further details as regards security of IT systems, please refer to the ICT Policy.

7. SUBJECT ACCESS REQUESTS

7.1. Anybody who makes a request to see any personal information held about them by the Charity is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).

7.2. All requests should be sent to Director of Operations and Finance within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

7.3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Director of Operations and Finance must, however, be satisfied that:

7.3.1. the child or young person lacks sufficient understanding; and

7.3.2. the request made on behalf of the child or young person is in their interests.

7.4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Charity must have written evidence that the individual has authorised the person to make the application and the Director of Operations and Finance must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

7.5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

7.6. A subject access request must be made in writing. The Charity may ask for any further information reasonably required to locate the information.

7.7. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be

appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

7.8. All files must be reviewed by Director of Operations and Finance before any disclosure takes place. Access will not be granted before this review has taken place.

7.9. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Exemptions to Access by Data Subjects

7.10. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

8. OTHER RIGHTS OF INDIVIDUALS

8.1. The Charity has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Charity will comply with the rights to:

8.1.1. object to processing;

8.1.2. rectification;

8.1.3. erasure; and

8.1.4. data portability.

Right to object to processing

8.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

8.3. Where such an objection is made, it must be sent to Director of Operations and Finance within 2 working days of receipt, and Director of Operations and Finance will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

8.4. Director of Operations and Finance shall be responsible for notifying the individual of the outcome of their assessment within 5 of working days of receipt of the objection.

8.5. Where personal data is being processed for direct marketing purposes an individual has the right to object at any time to processing of personal data concerning him or her for such marketing (which includes profiling to the extent that it is related to such direct marketing) and their personal data shall no longer be processed by the Charity for direct marketing purposes.

Right to rectification

8.6. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to Director of Operations and Finance within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

8.7. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall

be given the option of [a review under the complaints procedure, or] an appeal direct to the Information Commissioner.

8.8. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

8.9. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

8.9.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

8.9.2. where consent is withdrawn and there is no other legal basis for the processing;

8.9.3. where an objection has been raised under the right to object, and found to be legitimate;

8.9.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

8.9.5. where there is a legal obligation on the Charity to delete.

8.10. Director of Operations and Finance will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

8.11. In the following circumstances, processing of an individual's personal data may be restricted:

8.11.1. where the accuracy of data has been contested, during the period when the Charity is attempting to verify the accuracy of the data;

8.11.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

8.11.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

8.11.4. where there has been an objection made under 8.2 above, pending the outcome of any decision.

Right to portability

8.12. If an individual wants to send their personal data to another organisation they have a right to request that you provide their information in a structured, commonly used, and machine readable format. If a request for this is made, it should be forwarded to Director of Operations and Finance within 2 working days of receipt, and Director of Operations and Finance will review and revert as necessary.

9. BREACH OF ANY REQUIREMENT OF THE GDPR

9.1. Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to Director of Operations and Finance.

9.2. Once notified, the Director of Operations and Finance shall assess:

9.2.1. the extent of the breach;

9.2.2. the risks to the data subjects as a consequence of the breach;

9.2.3. any security measures in place that will protect the information;

9.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

9.3. Unless Director of Operations and Finance concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Charity, unless a delay can be justified.

9.4. The Information Commissioner shall be told:

9.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

9.4.2. the contact point for any enquiries (which shall usually be Director of Operations and Finance);

9.4.3. the likely consequences of the breach;

9.4.4. measures proposed or already taken to address the breach.

9.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then Director of Operations and Finance shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

9.6. Data subjects shall be told:

9.6.1. the nature of the breach;

9.6.2. who to contact with any questions;

9.6.3. measures taken to mitigate any risks.

9.7. Director of Operations and Finance shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the SMT and a decision made about implementation of those recommendations.

10. CONTACT

10.1. If anyone has any concerns or questions in relation to this policy they should contact Director of Operations and Finance.

11.

Communication

12. All staff.

Monitoring and review

13. This policy must be reviewed annually by the Director of Operations & Finance and/or amended in accordance any legislation and guidelines when such changes come into force.

Links to other policies

- Data Retention Policy
- Privacy policy
- Privacy notice staff

Document control

What date was this policy last approved?	September 2017
Who was the approving body/postholder?	Director of Ops and Finance
When was this policy implemented?	April 2018
What is the version number?	2.0
What version or policy does this one supersede?	1
What consultation was undertaken when writing this policy? (key names and departments)	CEO and SMT
What is the date of review? (Maximum 2 years from last approval date)	April 2020
Which department does this policy originate from?	Operations
Who is the lead manager	Sharon Daley
Who is the author/contact person (if different from above)?	