freephone: 0800 246 5874
phasethornbury@gmail.com

PHASE Thornbury Data Management Policy

INDEX

1. Purpose

1.1 The purpose of the policy is to set out how Phase manages the collection, retention, use of and disposal of data, documents and other information.

1.2 Complying with this policy is important not only in order for Phase to meet its legal obligations, but also to ensure that everyone we hold data on; whether young people and their families, staff, volunteers, trustees or anyone else; is treated fairly through the holding of that data, the way it is used and the manner in which it is disposed of.

1.3 Ensuring the efficient and effective management of data plays a key part in supporting Phase achieve its' strategic and operational objectives.

1.4 The person in Phase who has the primary responsibility for all matters relating to data is the Phase Operations Manager (OM). Anyone who requires advice and guidance on any issue relating to this policy, and its implementation, should consult with the Phase OM in the first instance.

2. Scope

2.1 This policy applies to all Phase activities and covers documents, data and photographs that are held in both electronic and paper format.

2.2 The policy incorporates Phase's responsibilities under legislation, primarily the Data Protection Act (2018), which incorporates the General Data Protection Regulations (2016)..

3. Principles

3.1 Personal data processed by Phase will abide by the general principles set out in the legislation. These principles are set out in Appendix A.

3.2 Anyone who has personal data held by Phase has a number of statutory rights. These are set out in Appendix B.

3.3 No personal data will be made available to any third party unless (a) there is a legal obligation to disclose it or (b) the relevant data subject has given approval to disclosure or (c) disclosure is considered to be in Phase's legitimate interest, which is not outweighed by any potential prejudice to the affected data subject's interests. This means, among other things, that we will not sell, or pass on, personal data purely for financial gain. However we do use the personal data we hold to contact data subjects with newsletters and these do include requests to support Phase in a number of ways, including financially.

4. Responsibilities

4.1 Trustees

The trustees are responsible for ensuring that Phase has an effective policy on data management and that it is regularly reviewed.

4.2 All Staff and volunteers

Staff and volunteers are responsible for:

i) Ensuring that Phase related personal data, held by them and about them, is accurate and up to date;

ii) Informing the appropriate person of (a) any failure to comply with this policy that they become aware of.

5. Data held

5.1 Volunteers, staff, trustees and contractors (where these are individuals)

- Address & contact details (phone numbers and personal email addresses)
- Relevant education, training and career experience
- DBS
- References
- Bank details (only paid staff and anyone receiving expenses)

Methods of collection : Phase application forms, directly from individuals

5.2 Service users

- Address & contact details (phone numbers and personal email addresses)
- Parent/carer names & contact details
- Health issues (relevant to Phase service delivery)
- Self assessment, agreed action plans etc as part of record of meetings

Methods of collection : Phase referral forms, directly from young person

5.3 Supporters/Donors(as they relate to individuals)

- Address & contact details (phone numbers and organisational/personal email addresses)
- Record of gifts

Methods of collection : Emails, web-site, correspondence, directly from individuals

6. Management of data

6.1 All Phase volunteers, staff and trustees, as part of their recruitment process, must complete a data management declaration which will confirm:

a) That they have read and understood the Data Management Policy and are willing to abide by it;

b) They will set up and use exclusively a Phase email address for all Phase related business;

c) That wherever Phase standard documents exist, that they will use these documents for recording personal data; and

d) That they will treat all Phase related personal data as confidential and will not share, or make available, this data with anyone unless authorised by the Phase Operations Manager (OM)or Trustees.

6.2 All volunteers, staff and trustees should immediately notify the Phase OM of any instance where personal data has (or may have) been accessed, or made available, to any authorised person or organisation.

6.3 Phase will provide information (and training wherever possible) on data management, to all those covered by this policy, whenever appropriate.

7. Data security

7.1 Paper records

7.1.1 Hard copies of records containing personal data should only be kept if (a) it is not practical to convert to an electronic record; or (b) there is a specific reason for keeping card copies.

7.1.2 Paper documents containing personal data should be kept in locked storage.

7.2 Email

7.2.1 All electronic communication on Phase business should be done using Phase emails. Emails have a great deal of potential for creating unintended records of personal data. The possible location of such records should be kept to a minimum.

7.2.2 All Phase volunteers, staff and trustees should regularly review saved emails and delete any that contain personal data unless the holding of that data is consistent with the DM Policy.

7.3 Electronic records

7.3.1 All devices being used to hold Phase related documents containing personal data should be password protected (including internet access).

7.3.2 As far as they exist, all records must be kept using Phase agreed formats.

8. Meeting our obligations under the Data Protection Act (2018)

8.1 Duties under the Act

8.1.1 The legislation governs the collection, storage, processing, disclosure and disposal of personal data. Some types of personal data are categorised as

special. However the only type of special data that Phase might hold is on ethnicity. This would be for the purpose of monitoring that Phase's services are provided without discrimination and/or to meet any contractual obligations from funders.

8.1.2 In order to comply with the legislation, Phase is required to identify the types of personal data that it holds and to show that, for each type, it has met its obligation namely:

i) That it has determined the legal basis for processing the data (see Appendix B);

ii) That the DP principles (Appendix A) have been met;

iii) That the data subjects concerned have been properly informed (Appendix C);

iv) That the data is kept in an appropriately secure environment; and

v) That the data is being effectively managed so that it remains accurate and up to date and that it is disposed of when it is no longer required.

8.1.3 In addition to the management of the personal data it processes, the following sections address how Phase meets these further requirements:

i) The rights of data subjects (the person to which the data refers) ; and

ii) Subject Access Requests.

8.2 Consequences of a failure to comply

8.2.1 Data security is increasingly recognised as a major issue, and numerous high profile cases, including the misuse of data by some charities in their fundraising activities, have put this subject very firmly in the public spotlight. The intensity of interest in this is only likely to grow and, consequently, so will the negative impact on an organisation's reputation of any failure to manage its data effectively.

8.2.2 The Information Commissioners Office (ICO), the body responsible for overseeing compliance with data protection, has powers to levy fines on organisations for failures.

8.3 Rights of data subjects

8.3.1 Phase, through this Data Management Policy and appropriate training, is committed to ensuring that all staff/volunteers understand their responsibilities as far as the rights of data subjects are concerned.

8.3.2 Under the legislation there are a number of specific rights, outlined below, that may be relevant in dealing with data subjects:

i) The right to be informed - there should be an agreed way that the data subject is told about the collection and use of their data;

ii) The right of access - the right of any data subject to be given the data held on them;

iii) The right to rectification - the right to have incorrect data changed;

iv) The right to erasure - this has to be balanced against the legitimate needs of Phase.

v) The right to restrict processing - exists in specific circumstances and again has to be balanced against the legitimate needs of Phase; and

vi) The right to object to the processing of data for (a) the legitimate purposes of Phase and (b) for direct marketing. In the case of the first Phase can refuse if the needs of the organisation outweigh those of the individual. In the case of the second Phase cannot refuse the request.

8.4 Subject access requests

8.4.1 Access requests can be made by anyone for whom Phase holds personal data.

8.4.2 Requests should be forwarded to the Phase Operations Manager (OM) in writing (email is acceptable). The OM will take reasonable steps to verify that the request has actually come from the data subject concerned.

8.4.3 The OM will seek to engage with the data subject as to the scope of the request if there is any doubt as to the actual data being requested. Phase is committed to providing, wherever possible, the information that is actually required rather than simply relying on the wording of the request.

8.4.4 Requests will be replied to within the statutory period of one month. Where possible the response time will be less than this. In exceptional cases the time limit can be extended by up to two months if it is a multiple and/or very complex request.

8.4.5 Under legislation the data subject is entitled to be given:

i) A copy of all of the records held;

ii) A description of the data held;

iii) The reason(s) for the data being processed;

iv) The origin of the data (if not provided by them);

v) Who has been given the data or who may be given it; and

vi) How long the data is expected to be kept.

8.4.6 Any data subject who is not content with the accuracy or completeness of the response to their request for information has the right to appeal to the trustees, within 10 working days of receipt of the response to their original request.

8.4.7 If the data subject is not satisfied with the response from the trustees then they will be advised of their right to complain to the Information Commissioner's Office.

<table>
<tr><td rowspan="4">This policy has been reviewed and approved by</td><td rowspan="2">Name (Position):</td><td>Signed:</td></tr>
<tr><td>Date:</td></tr>
<tr><td rowspan="2">Name (Position):</td><td>Signed:</td></tr>
<tr><td>Date:</td></tr>
<tr><td colspan="3">Policy to be reviewed:</td></tr>
</table>

Appendix A

The Data Protection General Principles under GDPR

1. Lawfulness, fairness and transparency
Organisations need to ensure their data collection practices don't break the law and that they aren't hiding anything from data subjects.

2. Purpose limitation
Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

3. Data minimisation
Organisations must only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits.

First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data.

Second, data minimisation makes it easier to keep data accurate and up to date.

4. Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

5. Storage limitation

Similarly, organisations need to delete personal data when it's no longer necessary.

6. Integrity and confidentiality

This is the only principle that deals explicitly with security. The GDPR states that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The seventh principle

The GDPR includes an additional principle, accountability, which acts as an overarching set of requirements related to the other six.

By achieving accountability, organisations demonstrate that they have the necessary documentation to prove that they are meeting their compliance requirements.

Appendix B

Rights of individuals who have personal data held by an organisation

Under the Data Protection legislation, data subjects (the person to which the personal data refers) have the following rights with regards to their personal information:

- the right to be informed about the collection and the use of their personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner

(Note - for more information refer to the Information Commissioner's web-site : www.ico.org.uk)

Appendix C

The legal basis for holding personal data

For each type of personal data held there must be one of the following legitimate legal basis for processing that data:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject (or to take steps to enter in to a contract with the data subject)
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject (or another person)
- Processing is necessary to fulfil the legitimate purposes of organisation, except where such interests are overridden by the interests, rights or freedoms of the data subject

Appendix D

Phase Data Protection Privacy Notice

Phase processes personal data relating to its staff as part of its normal operational activities. Personal data is any information that can be identified to a specific, living individual and processing means collecting, holding or using that information. Phased is based in Thornbury.

The person in Phase who is responsible for all matters relating to data is Marie Isles, Operations Manager. Marie can be contacted by email marie.phasethornbury@gmail.com. If you have any concerns about your personal data then please contact Marie.

Phase holds personal data on the following groups: staff, volunteers, trustees, contractors, young people (who receive Phase services) and supporters.

The reasons for collecting this personal data (and the legal basis for doing so) is:

Staff - to fulfil our obligations as an employer. The legal basis for collecting this data is that it is necessary for the performance of the contract of employment. This data will normally be kept for 6 years after the individual leaves the employment of Phase.

Volunteers/trustees - to ensure that trustees/volunteers are able to work effectively and safely as possible on behalf of Phase. The legal basis for collecting this data is that it is necessary to fulfil the legitimate purpose of Phase. This data will be kept for up to 12 months after the individual ceases to volunteer or steps down from being a trustee.

Contractors - to enable Phase to have access to the most appropriate professional services required by the young people we help. The legal basis for collecting this data is that it is necessary to fulfil the legitimate purpose of Phase. This data will

only be kept whilst the contractor concerned is a potential provider of professional services.

Young people (who receive Phase services) - to ensure that we are able to provide the best service possible. The legal basis for collecting this data is to protect the vital interests of the data subjects. This data will be kept until the young person reaches the age of 18 or leaves the area served by Phase.

Supporters - in order to maximise the capacity of Phase to meet the needs of young people, and their families. The legal basis for collecting this data is with the data subject's consent. This data will be kept until consent is withdrawn.

Personal data will only be shared with organisations that have a statutory right to see the relevant information. We will not share it with anyone for the purpose of sales or marketing without obtaining your consent to do so.

Under UK legislation there are a number of principles that apply to all types of personal data. The individual, to whom the data refers, also has a number of rights concerning their data. More information about both of these things can be found on the ICO's web-site www.ico.org.uk.