**PHAB NOTTINGHAM**

**DATA PROTECTION POLICY**

**LAST UPDATED: 16TH MAY 2018**

## 1. Introduction

This Policy sets out the obligations of Phab Nottingham, a Charity registered in England and Wales under Charity number 1153383, whose registered office is at 82 Wandsworth Bridge Road, London, SW6 2TF ("the Charity") regarding data protection and the rights of its service users a.k.a "Members" ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR"). As all our Members are children/vulnerable adults, the rights of the "data subjects" conveyed in this Policy shall be in practice executed by their parents/legal guardians.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person 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 natural person.

This Policy sets the Charity's obligations regarding the collection, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Charity, its employees, agents, contractors, or other parties working on behalf of the Charity.

The Charity is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## 2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

2.6 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.

## 3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 11).

3.2 The right of access (Part 12);

3.3 The right to rectification (Part 13);

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 14);

3.5 The right to restrict processing (Part 16);

3.6 The right to data portability (N/A);

3.7 The right to object (N/A); and

3.8 Rights with respect to automated decision-making and profiling (N/A).

## 4. Specified, Explicit, and Legitimate Purposes

4.1 The Charity collects and processes the personal data set out in Part 15 of this Policy. This includes:

4.1.1 Personal data collected directly from data subjects or their legal guardians

4.2 The Charity only collects, processes, and holds personal data for the specific purposes set out in Part 15 of this Policy (or for other purposes expressly permitted by the GDPR).

4.3 Data subjects are kept informed at all times of the purpose or purposes for which the Charity uses their personal data. Please refer to Part 10 for more information on keeping data subjects informed.

5. **Adequate, Relevant, and Limited Data Processing**

The Charity will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 10, below.

6. **Accuracy of Data and Keeping Data Up-to-Date**

6.1 The Charity shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 12, below.

6.2 The accuracy of personal data shall be checked when it is collected and at 24 month intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

6.3 Data subjects/their legal guardians shall be provided with regular opportunities to update their personal data.

7. **Data Retention**

7.1 The Charity shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected and held.

7.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

7.3.1 The objectives and requirements of the Charity;

7.3.2 The type of personal data in question;

7.3.3 The purpose(s) for which the data in question is collected and held;

7.3.4 The Charity's legal basis for collecting and holding that data;

7.3.5 The category or categories of data subject to whom the data relates;

7.3.6 The limitation period for any claims of personal injury or negligence for which the personal data may be of material relevance (currently six years in UK);

7.3.7 Requirements of any insurance policies undertaken.

7.4 If a precise retention period cannot be fixed for a particular type of data,

criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the defined retention periods set out below, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Charity to do so (whether in response to a request by a data subject or otherwise).

7.6 Relevant personal data contained in Application Forms and volunteer feedback forms may be retained for the claim limitation period in case of any significant incidents reported.

## 8. Data Disposal

8.1 Upon the expiry of the data retention periods set out below in Part 8 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

8.1.1 Personal data stored electronically (including any and all backups thereof) shall be deleted;

8.1.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted;

8.1.3 Personal data stored in hardcopy form shall be shredded;

8.1.4 Special category personal data stored in hardcopy form shall be shredded.

## 9. Secure Processing

The Charity shall ensure that all personal data collected and held is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 16 to 23 of this Policy.

## 10. Keeping Data Subjects Informed

10.1 The Charity shall provide the information set out in Part 10.2 to every data subject:

10.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

10.2 The following information shall be provided:

10.2.1 Details of the Charity

10.2.2 The purpose(s) for which the personal data is being collected (as detailed in Part 15 of this Policy) and the legal basis justifying that collection;

10.2.3 Where applicable, the legitimate interests upon which the Charity is justifying its collection of the personal data;

10.2.4 Details of data retention;

10.2.5 Details of the data subject's rights under the GDPR;

10.2.6 Details of the data subject's right to withdraw their consent to the Charity's processing of their personal data at any time;

10.2.7 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR)

## 11. Data Subject Access

11.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Charity holds about them, what it is doing with that personal data, and why.

11.2 Data subjects wishing to make a SAR should do using a Subject Access Request Form, sending the form to dataprotection@phabnottingham.co.uk

11.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

11.4 The Charity does not charge a fee for the handling of normal SARs. The Charity reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 12. Rectification of Personal Data

12.1 Data subjects have the right to require the Charity to rectify any of their personal data that is inaccurate or incomplete.

12.2 The Charity shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Charity of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

12.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## 13. Erasure of Personal Data

13.1 Data subjects have the right to request that the Charity erases the personal data it holds about them in the following circumstances:

13.1.1 It is no longer necessary for the Charity to hold that personal data with respect to the purpose(s) for which it was originally collected;

13.1.2 The data subject wishes to withdraw their consent to the Charity holding their personal data;

13.1.3 The data subject objects to the Charity holding their personal data (and there is no overriding legitimate interest to allow the Charity to continue doing so including, but not limited to, those detailed in Part 7 of this Policy);

13.1.4 The personal data has been processed unlawfully;

13.1.5 The personal data needs to be erased in order for the Charity to comply with a particular legal obligation**.**

13.2 Unless the Charity has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

13.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 14. Personal Data Collected and Held

The following personal data is collected and held by the Charity (for details of data retention, please refer to Part 7 of this Policy):

| Data Ref. | Type of Data | Purpose of Data |
|---|---|---|
| 001 | Personal and special category data provided by data | To enable the preparation and provision of care for the data subject and ability to ensure their welfare in case of emergency. |

| Data Ref. | Type of Data | Purpose of Data |
|---|---|---|
| | subject/legal guardian via Application Form | |
| 002 | Personal data in the form of behavioural/health observations made by Volunteers through feedback forms | To enable the preparation and provision of care for the data subject. |
| 003 | Personal and special category data provided by data subject/legal guardian via phone call and noted in appendices to their Application Form. | To enable the preparation and provision of care for the data subject and ability to ensure their welfare in case of emergency. |

15. **Data Security - Transferring Personal Data and Communications**

The Charity shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

15.1 When sending personal data internally, the data itself should be stored securely on OneDrive in an appropriately labelled folder and a link provided to the recipient (requiring password-protected login to view);

15.2 When receiving personal data, the data should be copied from the body of that email and stored securely on OneDrive together with any attachments. The email itself should be deleted. All temporary files associated therewith should also be deleted. When replying to the email, the personal data should be first removed from the original email. If other contents of the email is required to be retained for reference, it may be saved in a folder labelled 'Correspondence' on OneDrive;

15.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

15.4 Personal data contained in the body of an email and attachments, whether sent or received, should be sent/received through a Phab Nottingham email address;

15.5 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;

15.6 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

## 16. Data Security - Storage

The Charity shall ensure that the following measures are taken with respect to the storage of personal data:

16.1 All electronic copies of personal data should be stored securely on OneDrive (requiring password-protected login to view);

16.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar other than when in the possession of Volunteers on events in which case the measures detailed in 16.5 will be followed;

16.3 No personal data should be stored locally on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Charity or otherwise without the formal written approval of the Board of Trustees and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

16.4 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Charity where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Charity that all suitable technical and organisational measures have been taken).

16.5 When personal data is shared with Volunteers, it is done only via hardcopy, copies are signed-in and out at the end of each day and stored securely in a backpack unless in-use.

## 17. Data Security - Disposal

17.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to Part 7 of this Policy.

18. **Data Security - Use of Personal Data**

The Charity shall ensure that the following measures are taken with respect to the use of personal data:

18.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Charity requires access to any personal data that they do not already have access to, such access should be formally requested from the Board of Trustees;

18.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Charity or not, without the authorisation of the Board of Trustees;

18.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

18.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

18.5 Where personal data held by the Charity is used for marketing purposes, it shall be the responsibility of the Publicity Officer of the Management Committee to ensure that the appropriate consent is obtained.

19. **Data Security - IT Security**

The Charity shall ensure that the following measures are taken with respect to IT and information security:

19.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

19.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Charity, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

20. **Organisational Measures**

The Charity shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

20.1 All employees, agents, contractors, or other parties working on behalf of the Charity shall be made fully aware of both their individual responsibilities and the Charity's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

20.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Charity that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Charity;

20.3 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately trained to do so;

20.4 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be appropriately supervised;

20.5 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

20.6 Methods of collecting and holding personal data shall be regularly evaluated and reviewed;

20.7 All personal data held by the Charity shall be reviewed periodically;

20.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Charity handling personal data shall be regularly evaluated and reviewed;

20.9 All employees, agents, contractors, or other parties working on behalf of the Charity handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

20.10 All agents, contractors, or other parties working on behalf of the Charity handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Charity arising out of this Policy and the GDPR; and

20.11 Where any agent, contractor or other party working on behalf of the Charity handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Charity against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 21. Data Breach Notification

21.1 All personal data breaches must be reported immediately to the Board of

Trustees.

21.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Board of Trustees must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

21.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 21.2) to the rights and freedoms of data subjects, the Board of Trustees must ensure that all affected data subjects are informed of the breach directly and without undue delay.

21.4 Data breach notifications shall include the following information:

21.4.1 The categories and approximate number of data subjects concerned;

21.4.2 The categories and approximate number of personal data records concerned;

21.4.3 The name and contact details of a contact point from whom more information can be obtained);

21.4.4 The likely consequences of the breach;

21.4.5 Details of the measures taken, or proposed to be taken, by the Charity to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## 22. Implementation of Policy

This Policy shall be deemed effective as of the date indicated at the head of this document. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.