Data Protection Policy

Introduction
In order to comply with data protection law, we will ask for consent and inform those giving us their personal data about our usage of that data; we know what data we hold and why we are keeping it, we store and transport the data encrypted, and we will delete the data when it is no longer required. We have a procedure to respond to any subject access requests and to respond to breaches of data protection.

1) Consent
When we collect the data, we will inform applicants, peer supporters and workshop attendees of why we keep their data and for how long. We do not collect personal data belonging to those who receive support at our support groups.

2) What data we keep and why
We will collect the minimum data we need and hold it only for the minimum time we need.

We hold
a) **peer supporter** names, email addresses, which training has been completed, and in what activity each peer supporter is currently involved. We hold this data to communicate with our peer supporters, to ensure that they have met their ongoing training requirements, and to inform them of meetings, fund raising events, training and other Treasure Chest news.
b) a list of **peer supporter** Disclosure and Barring Service (DBS) certification, with name and certificate numbers in order to ensure all DBS certificates and responsibilities are up to date.
c) names, addresses and email addresses of **prospective applicants and applicants**; we also hold notes relevant to their prospective application (such as if they are training to be a professional health worker) and their application form, in order to evaluate their suitability to be a peer supporter and to communicate regarding training.
d) names, email addresses, phone numbers and “due dates” of **end-users attending antenatal workshops**, in order to communicate with them in the run up to the workshop, and to offer support once their baby is born.

3) Storage and sharing
Digital data will only be stored, shared (e.g. by e-mail) and transported encrypted. These standards apply also to any backup copies of the data. For storage, an encrypted device (e.g. phone, tablet, PC) or encrypted container within a device should be used. For transfer and backups, a password-protected, encrypted zip file (or something of equivalent security) will be used.

Passwords/pass phrases allowing access to the data will be kept securely, not shared with any person who does not have a legitimate need to access the data, not be the same as used for any other service, not be stored or transmitted along with the data being protected, and be at least 12 characters in length.

Hard copies of data will be stored in a locked container, e.g. locked filing system.

Those who do not need access to the data to perform a legitimate function of Treasure Chest will not be given it.

4) How long we keep data. When we delete it.
We keep peer supporter data while each peer supporter is active. Data is deleted once a peer supporter leaves the organisation. Every year the secretary will ascertain whether peer supporters are active. If not, data will be deleted. The same applies to peer supporter DBS records, and to prospective peer supporter records, in which case the DBS co-ordinators and course co-ordinators will delete data.

Antenatal workshop attendees' records are kept until after their child is born. Every year the antenatal workshop co-ordinator will check for and delete old data.

Hard copies of data will be shredded.

5) Procedure for Subject Access Requests
Any individual has a right to request a copy of the data we hold about them. We will respond to subject access requests within 30 days, and make no charge.

In order to ensure we only release data to the correct person, we will:
- respond to subject access requests using contact details already known to us
- ask for a small piece of (non-public) information already known to us (such as which antenatal workshop was attended, or which group a peer supporter supported) to ensure the identity of the requester is not in doubt
- in the unlikely event their identity is still in doubt we would ask to meet to see a form of identification.

6) Personal data breaches[1]
Personal data breaches can include:

- access to personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

As soon as a Peer Supporter becomes aware of a personal data breach, they must inform the Core Committee. As a minimum the Core Committee will inform the individual(s) whose personal data has been breached. In circumstances where it is felt that a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the breach will be reported to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

A record will be kept of all data breaches, regardless of whether there was a need to report to the Information Commissioner's Office.

[1] For more information, see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa

6) Updates
This policy will be reviewed once every three years to assess if it is still fit for purpose, and to make any updates.

Responsibilities
The Treasure Chest Secretary will liaise with trainers and the wider Committee to ensure that this policy is circulated to all peer supporters on completion of their training.

It is the responsibility of individual peer supporters to familiarise themselves with this policy and to read and understand its content.

Date of last review: November 2020
Reviewed by: Kath Weston
Date of next review: November 2023