BLACKDOWN Support GROUP

REG CHARITY 1013514

Data Protection Policy

Last updated	August 2018

Definitions

Charity	means Blackdown Support Group, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Charity Co-ordinator
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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."

2. General provisions

a. This policy applies to all personal data processed by the Charity.

b. The Chair of Trustees shall take responsibility for the Charity's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

d. The Charity shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

b. The Charity shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

5. Data minimisation

a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. Paper records should be retained for the following periods at the end of which they should be shredded:

   i. Client records – 6 years after ceasing to be a client.

   ii. Staff records – 6 years after ceasing to be a member of staff.

   iii. Unsuccessful staff application forms – 6 months after vacancy closing date.

   iv. Volunteer records – 6 years after ceasing to be a volunteer.

   v. Timesheets and other financial documents – 7 years.

   vi. Employer's liability insurance – 40 years.

c. Archived records should clearly display the destruction date.

8. Security

a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

b. If you discover, or suspect, a data protection breach you should report this to the BSG Co-ordinator who will review our systems, in conjunction with the Data Protection Trustee, to prevent a reoccurrence. The chair of trustees should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the board of Trustees. There is a time limit for reporting breaches to ICO so the Chair of trustees should be informed without delay.

10. The Rights of an Individual

a. Data subjects can ask, in writing to the chair of trustees, to see all personal data held on them, including e-mails and computer or paper files. The data processor (BSG) must comply with such requests within 30 days of receipt of the written requests.

END OF POLICY

Advice on Confidentiality

- *All information about clients held by Blackdown Support Group is strictly confidential*
- *Be aware that careless talk can lead to a breach of confidentiality – discuss your work only with the Co-ordinator, preferably in private.*
- *Always keep confidential documents away from prying eyes.*
- *Verbal reporting should be carried out in private. If this is not possible, it should be delivered in a volume such that it can only be heard by those for whom it is intended.*
- *When asking for confidential information in circumstances where the conversation can be overheard by others conduct the interview in as quiet and discreet a manner as possible and preferably find somewhere private for the discussion.*
- *Do not disclose personal information learnt in the course of your work.*

Review Date: August 2018

Approved by Committee on:12th March 2019

Signed by Chairman: Vicky Norton

Next review date: March 2020