Blackdown Support Group

'Supporting Lives, Strengthening Communities'

Charity No: 1208925

DATA PROTECTION POLICY

DEFINITIONS

Register of Systems:	A register of all systems or contexts in which personal data is processed by the Blackdown Support Group
Data Subject:	The identified or identifiable living individual to whom personal data relates.
Data Controller:	A person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the case of the BSG the Data Controller is the Chair of the Board of Trustees.

DATA PROTECTION PRINCIPLES

The Blackdown Support Group (BSG) is committed to processing data in accordance with its responsibilities under the General Data Protection Regulations (GDPR), as enacted in the Data Protection Act 2018.

Article 5 of 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 incompatible with those purposes.
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
d. Accurate and up to date.
e. Kept in a form which permits identification of data subjects for no longer than is necessary and 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.

GENERAL PROVISIONS

a. This policy applies to all personal data processed by the BSG including, but not limited to:
    i. Employees

ii. Unsuccessful candidates for employment
iii. Volunteers
iv. Service-Users
v. Friends and Donors
vi. Independent Service-Providers

b. The Chair of the Board of Trustees shall take responsibility for the ongoing compliance with this policy
c. This policy shall be reviewed 3 yearly or sooner should legislation change
d. The BSG is registered with the Information Commissioner's Office as an organisation that processes personal data

LAWFUL, FAIR AND TRANSPARENT PROCESSING

a. To ensure the processing of data is lawful, fair, and transparent, a Register of Systems (see Appendix 1) shall be maintained and reviewed at least annually
   i. Paper records for Volunteers
   ii. Paper records for Service Users
   iii. Internal Databases
   iv. External Databases
b. Individuals have the right to access their personal data and any such request shall be dealt with in a timely manner. This will normally be within one calendar month but, where a Subject Access Request (SAR) is particularly complex, may be extended up to two calendar months[1].

LAWFUL PUROSES

a. All data held by the BSG must be processed on the lawful basis of consent and noted in the Register of Systems
   i. Volunteers. When newly recruited, volunteers are asked to sign a declaration that they have read our privacy statement and that they are happy for their data to be kept by the organisation. They are informed of their right to withdraw consent at any time.
   ii. Service-users are asked their details at the time of registration. Details are recorded electronically on Optimise (or such external database as BSG is using at the time) and they are asked to provide verbal consent for data to be stored at the time. Optimise will flag up situations where consent has not been requested verbally or recorded.
   iii. Mailing lists are maintained for all volunteers, for all volunteer drivers and for friends.
b. Where communications are sent to individuals based on their consent the option for the individual to revoke their consent should be clearly visible and systems in place to ensure revocation is affected and accurately recorded.

DATA MINIMISATION

The BSG shall ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This will be achieved by ensuring that, whenever a decision is made to capture or record new data about individuals, careful consideration is given to what data will be recorded before it is requested. A procedure for data minimisation can be found at Appendix 3.

[1] Subject Access Requests (SAR)- Organisations must respond to a SAR within one month of receipt of the request. However, this could be extended by up to two months if the SAR is complex.

ACCURACY

Reasonable steps shall be taken to ensure personal data is accurate and up to date

ARCHIVING / REMOVAL

To ensure personal data is not kept for longer than necessary an archiving procedure is in place and will be reviewed annually (see Appendix 5).
Paper records should be retained for the following periods after which they will be shredded:

a. Service-user records: six years after ceasing to be a service-user
b. Staff records: six years after ceasing to be a member of staff
c. Unsuccessful staff application forms: six months after vacancy closing date
d. Volunteer records: six years after ceasing to be a volunteer
e. Timesheets and other financial documents: seven years
f. Employer's Liability Insurance certificates: 40 years

Archived records should clearly display the intended destruction date.

SECURITY

a. Paper records are kept locked in a cabinet with limited keyholder access, within an office that is locked when not in use.
b. All electronic records will be stored securely using modern up-to-date software restricted by password access.
c. Access to personal data shall be limited to personnel who need access and appropriate security in place to avoid unauthorised sharing of information
d. When personal data is deleted in accordance with the Archiving / Removal provisions above it shall be done in such a way that the data is irrecoverable
e. Appropriate back-up and disaster recovery solutions shall be in place

BREACH

a. Any breach of security affecting personal data shall be promptly assessed in relation to people's rights and freedoms and if necessary, reported to the Information Commissioner's Office.
b. Anyone suspecting or discovering any data protection breach must report this immediately to the Manager who will, with the Chair of the Board of Trustees, investigate and review our systems. **NB**: There is a time limit for reporting breaches to ICO so either the Chair or Manager should be informed as a matter of urgency.

RIGHTS OF INDIVIDUAL

Data subjects can ask, in writing to the Chair of the Board of Trustees, to see all personal data held on them including emails and computer or paper files. The BSG must comply with such requests at the earliest opportunity and within 30 days of receipt of the written request unless there are unusual complexities.

Review Date: April 2024

Approved by Trustees on: 16th July 2024

Signed by Chairperson: 

Next Review Date: July 2027

Appendix 1 Register of systems

Introduction

In accordance with the General Data Protection Regulation, this document sets out the approach of the Blackdown Support Group to the collection, use and management of the personal data under the following headings:

• Purpose for which the data are used

The data we collect and in what way

• How the data are stored and who has access to them

• Sharing the data

• Data removal and archiving

Purpose for which the data are used

The data collected is processed based on Legitimate Interest.

The data collected and in what way

On contacting The Blackdown Support Group via telephone, online or post, individuals are asked details to complete an enquiry form and to supply name and email address, a residential address and telephone number.

This data is entered on to an Excel spreadsheet and updated as required throughout the lifecycle of the project or as new data is made available (e.g. change of email or residential address).

Enquiries where no further action is deemed necessary are deleted.

The Blackdown Support Group website also provides an option to contact us. The Manager and employed staff have access to this and have responsibility for using details supplied to amend and maintain this database.

See Appendix 2 for details of precisely what information is retained by BSG in relation to different categories of data subject

How the data are stored and who has access to them

See Appendix 4

Sharing the data

See Appendix 4

Data removal and archiving

See Appendix 5

Appendix 2 Categories of Data routinely held and processed by BSG

	Employees	Unsuccessful Employees	Volunteers	Service-Users	Friends and Donors
Name	√	√	√	√	√
Address	√	√	√	√	√
Telephone No.	√	√	√	√	√
Email	√	√	√	√	√
D.O.B	√	√	√		
References	√	√	√		
Payroll Information	√		√		
Pension Information	√				
Contract of Employment	√				
Health Record	√		√	√	
Emergency Contact	√		√	√	
Driver's Licence			√		
Tax Code	√				
National Insurance No.	√		√		

Special Category Information

The special categories are information about people's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic information;
- biometric information (where used for identification purposes);
- health;
- sex life; and
- sexual orientation.

We hold Special Category information for Staff, Volunteers, Service-Users.

Records of special category information about our employees are kept electronically on SharePoint and paper copies are stored away in a locked cabinet within a locked office.

Records of special category information about our Volunteers and Service Users are kept on our database system Optimise, and a physical paper copy, which is stored in a locked office in a locked cabinet which only current employees have access too.

This is information that is considered especially sensitive, and so is given a greater level of protection.

Appendix 3 Suggested procedure for ensuring minimisation of data capture and processing

1. The Manager, in consultation with the Chair of Trustees, will review annually data currently recorded for each system (paper, internal electronic and external electronic) and subject categories (employees, volunteers, service-users, friends, etc.

2. The Manager and Chair of Trustees will carefully consider the justification for inclusion of each category of data for the specific subject group.

3. Where it is agreed that data are superfluous to requirement, the following steps will be taken:

    a. Any proposed changes will be referred to the risk management sub-committee
    b. Subject to the agreement of the risk management sub-committee, the records will be amended as appropriate

Appendix 4 Procedure for ensuring security of data

How the data are stored and who has access to them

All staff at Blackdown Support Group have access to the personal data of service-users, potential service-users, Volunteers, friends, and donors. This access is via SharePoint, Email, Telephone, Post, Paper Records and via External Databases Optimise and Lamplight.

Employees' and Unsuccessful Employees' data are held on SharePoint; only current staff members have access to this.

Paper Records are stored in a locked office that only staff members have access to via a lock box, the code for which is only known to staff members. Access to the building in which the BSG office is located is through a key fob, which only staff members hold. The key fob is handed back on cessation of employment.

Where personal data are taken verbally (by telephone or in person) consented is secured verbally using the consent form at Appendix 6 below:

Where communication is by email, such messages routinely include the option to withdraw consent in the electronic signature for all employees as follows:

> If you no longer wish to receive emails from The Blackdown Support Group, please let us know and we will remove you from our mailing list.

The Blackdown Support Group use NHSmail, the secure email, collaboration and directory service. NHSmail is the national secure collaboration service for health and social care in England. It includes a full suite of collaboration and productivity tools based on Microsoft Office 365, such as Outlook for email and calendar, Teams for instant messaging and video calls, and Office for documents and spreadsheets. The benefits of NHSmail are:

- Improved communication between healthcare professionals and staff across the NHS
- reduces the risk of data breaches
- protects patient privacy
- is compatible with a wide range of devices and platforms

This access is rescinded should a staff member leave the employment of the charity.

Sharing the data

The complete data set is available to the employees of The Blackdown Support Group as required for them to be able to carry out their roles.

The complete data set will not be shared with any third party unless legally obliged to do so.

Emailing processes when using sensitive data (alternative to bcc)

- Ensure compliance with current policy provision. (See Appendix 7)

- Review any change in legal requirements
- Review following any breach

Appendix 5 Procedure for archiving or destroying data

Data removal and archiving

To ensure personal data is not kept for longer than necessary an archiving policy will be put in place and reviewed annually.

Paper records should be retained for the following periods after which they will be shredded:

a. Service-user records: six years after ceasing to be a service-user
b. Staff records: six years after ceasing to be a member of staff
c. Unsuccessful staff application forms: six months after vacancy closing date
d. Volunteer records: six years after ceasing to be a volunteer
e. Timesheets and other financial documents: seven years
f. Employer's Liability Insurance certificates: 40 years

Archived records should clearly display the intended destruction date.

The following procedure will be applied for the archiving and destruction of records:

1. **Paper Records**

- When the data subject is no longer actively involved with BSG, any paper records relating to them will be placed in a securely locked archive container with the date for intended destruction clearly identifiable.
- At least twice each year the archive will be checked in order to identify records scheduled for destruction.
- Documents will be shredded and bagged for secure disposal.

2. **Electronic records**

- When the data subject is no longer actively involved with BSG, any electronic record relating to them will be archived on Optimise or in a folder in SharePoint.
- At least twice each year the archive will be checked in order to identify records scheduled for destruction.
- Documents will be deleted off of the online database.

Appendix 6 Declarations of Consent

a. Volunteers - When newly recruited, volunteers are asked to sign a declaration that they have read our privacy statement and that they are happy for their data to be kept by the organisation. They are informed of their right to withdraw consent at any time.

(i) **I wish to offer my services to the Blackdown Support Group as a volunteer. I have read the Blackdown Support Group's Privacy Statement and give consent for the Blackdown Support Group to hold my personal information on file as described therein and to complete a DBS check on my behalf.**

Signed: ..... Date: .....

b. Service-users - are asked their details at the time of registration. Details are recorded electronically on Optimise and they are asked to provide verbal consent for data to be stored at the time. Optimise will flag up situations where consent has not been requested verbally or recorded.

Consent

(i) In order for us to help you, we need to record some of your personal details which may include sensitive data about your medical needs or personal circumstances. To comply with the Data Protection Act (1998) we must tell you how we will use this data and ask for your permission. By signing this form or giving your verbal consent, you are providing your permission for us to process your data for the purposes below.

(ii) Your data will be stored at the BSG office and accessed by our staff and volunteers only as necessary to provide you with the service or services which you receive.

(iii) We may need to share personal or special categories of personal information with other helping agencies on a need-to-know basis. This will not be done without your consent.

(iv) We will keep your personal data for six years following your ceasing to be a client or volunteer of the BSG.

(v) Your data will be stored securely on computers protected by a firewall and by passwords. Paper copies will be kept in a locked office within the Blackdown Practice.

(vi) You can choose to remove your consent to us keeping your data at any time by contacting the Co-ordinator. You will be made aware if your withdrawal of consent will affect the provision of services to you.

(vii) Yes - I give my consent to the Blackdown Support Group to record personal information about me.

(viii) No – I do not give my consent to the Blackdown Support Group to record personal information about me.

Signed/Verbal consent given Date

c. Mailing lists are maintained for all volunteers, for all volunteer drivers and for friends.

d. **Employees** - When newly recruited, employees are asked to sign a contract, this includes that they consent to the holding and processing of personal data provided by them to the Organisation as follows:

22. DATA PROTECTION ACT 1998:

For the purposes of the Data Protection Act 1998 you give your consent to the holding and processing of personal data provided by you to the Organisation for all purposes relating to the performance of your employment including, but not limited to:

- Administering and maintaining HR records;
- Paying and reviewing salary and other remuneration and benefits;
- Providing and administering benefits (including if relevant, pension, or insurance);
- Undertaking performance and fitness, appraisals and reviews;
- Maintaining sickness and other absence records;
- Providing references and information to future employers, and if necessary, governmental and quasi-governmental bodies for social security and other purposes, HM Revenue and Customs and the National Insurance Contributions Office;
- Providing information to future partner organisation or organisations with whom we may merge or transfer an undertaking to;
- Transferring information concerning you to a country or territory outside the EEA.

23. SENSITIVE PERSONAL DATA:

From time to time it may be necessary to process sensitive personal data, for example, information relating to an individual's ethnic origin for equal opportunity monitoring. By signing this contract you agree that the Organisation may retain and process sensitive personal data about you as the needs of the Organisation require.

Appendix 7 Email Policy

1. **Create strong passwords**

One of the most important email security best practices is to use strong passwords.

2. **Charity Password Policy**

Password requirements and expectations are that passwords should be long not complex to ensure password strength. Stringing together a few words such as kittEnsarEadorablE is one method to make longer, easy-to-remember yet difficult-to-guess passwords that help defend against attackers who use dictionary attacks to target weak passwords.

3. **Don't reuse passwords across accounts**

Password reuse is a major email security threat. If an attacker compromises one account that uses the same credentials as other accounts, the attacker can easily gain access to those other accounts. Attackers know that trying a reused password associated with a person's account on a breached system often unlocks other accounts. Password reuse is especially dangerous when employees use the same passwords for corporate and personal accounts.
Employees should use strong, unique passwords for each account.

4. **Changing passwords**

Password changes should be made following a suspected compromise or data breach.

5. **Use multifactor authentication (MFA)**

   MFA involves using more than one method to authenticate a user's identity. For example, a username and password in combination with a one-time password or fingerprint biometric. Adding a second -- or third, or more -- factor to the authentication process adds an additional layer of defense and defends against common email threats, such as brute-force attacks and password cracking. Microsoft has predicted locking down accounts with MFA can block 99.9% of account compromise attacks.

   MFA helps protect users by making it more difficult for someone else to sign in to their NHSmail account. It uses two different forms of identity: the user's password, and a secondary authentication method.

   Employees should also protect their personal accounts by using MFA wherever available.

6. **Phishing**

While email security products prevent many spam emails from reaching a user's inbox, a good amount of spam still gets through that can contain phishing schemes, which are becoming increasingly sophisticated. These can include standard phishing emails, along with spear phishing or whaling attacks. Users should be on the lookout for phishing scams and use caution when opening any potentially malicious emails. Don't open, respond to, click links in or open attachments from emails that appear suspicious.

7. **Be wary of email attachments**

Many email attacks rely on the ability to send and receive attachments that contain malicious executable code. Email security gateways and antimalware software can detect malicious sources and block most malicious attachments. These attachments, however, can also come from trusted sources that have been exploited by attackers.

Whatever the source, employees should beware of attachments even when the organization uses email-scanning and malware-blocking software. Use extra caution before opening an attachment that has an extension associated with an executable program, such as EXE (executable file), JAR (Java application file) or MSI (Windows Installer). Files such as Word documents, spreadsheets and PDFs can also carry malicious code, so be careful handling any type of attached file. Scan files with an antimalware program or avoid opening them altogether.

8. **Don't click email links**

Hyperlinks in emails can often connect to a web domain different from the one they appear to represent. Some links might display a recognizable domain name -- such as www.amazon.com -- but, in fact, direct the user to a different, malicious domain. Attackers also use international character sets or misspellings to create malicious domains that appear to be those of well-known brands.

Always review link contents by hovering the mouse pointer over the link to see if the actual link is different from the displayed link. Note that even this can be spoofed, however, though most modern email programs should catch such links. When in doubt, type domains directly into browsers to avoid clicking links in emails.

9. **Don't use business email for personal use and vice versa**

Blackdown Support Group prohibits the use of corporate email accounts for personal matters. Do not send work-related emails from personal accounts.

Mixing business and personal matters can result in threats such as spear phishing.

10. **Only use corporate email on approved devices**

People can access email from practically anywhere and on any internet-connected device. While convenient for employees, this could become a security disaster for an organization. If company email is opened on devices that don't have the proper security controls, attackers could exfiltrate users' credentials, email and data.

Employees must only access email on company-approved and trusted devices.

11. **Encrypt email, communications and attachments**

It has been said that email is like a postcard: Every person and system that it comes in contact with can see what is written. This is why email encryption is so important. Encryption, the process of converting plaintext into ciphertext, ensures that anyone who intercepts the email cannot read its contents. This helps prevent many email security issues, such as man-in-the-middle and business email compromise attacks. Most major email services have encryption capabilities.

Encrypting the message isn't enough on its own, however. Also encrypt communications between the organization and the email provider. Encrypt attachments as well, even if the email they are attached to is encrypted.

12. **Avoid public Wi-Fi**

Public Wi-Fi connections are ripe for attacks. If employees log into corporate email on public Wi-Fi, anyone on that network could also access their email. Malicious actors can use open source packet sniffers, such as Wireshark, to monitor and gain access to personal information via email. Even if users don't actively check email on public Wi-Fi, almost every system is set to automatically update inboxes when a device connects to a network. If users are on Wi-Fi, then so is their email, putting account credentials at risk.

Only use secure, known Wi-Fi networks to check email.

13. **Log out**

Employees are required to log out of their email when it's not in use and when they have finished for the day. Leaving email open on devices that are accessible to others can lead to security issues.