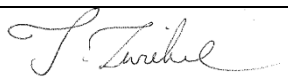
Sunbeams

DATA PROTECTION POLICY

Document Control Sheet

Document Title	Sunbeams Data Protection Policy
Document Reference	SBP10
Version Number	12
Date Created	September, 2014
Date Approved	September, 2025
Next Review Date	September, 2026
Status	Approved
Approved By	Jessica Zwiebel, Safeguarding Officer and Trustee
Signature	

Revision History

Version	Date	Author	Description of Change	Approved By
1.0	Sep 2014	Admin	Initial release outlining data protection principles.	Board of Trustees
2.0	Sep 2015	Admin	Review	Board of Trustees
3.0	Sep 2016	Admin	Review	Board of Trustees
4.0	Sep 2017	Admin	Review	Board of Trustees
5.0	Sep 2018	Admin	Minor GDPR-related alignment.	Board of Trustees
6.0	Sep 2019	Admin	Review	Board of Trustees
7.0	Sep 2020	Admin	Review	Board of Trustees
8.0	Sep 2021	Admin	Review	Board of Trustees
9.0	Sep 2022	Admin	Minor update to data breach procedure.	Board of Trustees
10.0	Sep 2023	Admin	Review	Board of Trustees
11.0	Sep 2024	Admin	Review	Board of Trustees
12.0	Sep 2025	Admin	Comprehensive annual review; refreshed layout and clarified consent definitions.	Board of Trustees

1. Policy Statement

Sunbeams is committed to protecting the rights and freedoms of individuals in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and where applicable, the Privacy and Electronic Communications Regulations (PECR) for marketing and fundraising activities.

We collect, store, and process personal data about service users, staff, volunteers, and supporters. We take data protection and confidentiality seriously and are committed to handling all personal information lawfully, fairly, and transparently.

2. Scope of the Policy

This policy applies to all staff, volunteers, trustees, contractors, and third parties who process personal data on behalf of Sunbeams.

3. Data Protection Principles

In accordance with the UK GDPR, Sunbeams ensures that personal data is:

1. **Lawfulness, fairness and transparency** – Processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation** – Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data minimisation** – Adequate, relevant and limited to what is necessary.
4. **Accuracy** – Accurate and kept up to date.
5. **Storage limitation** – Kept in a form which permits identification of data subjects for no longer than is necessary.
6. **Integrity and confidentiality** – Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
7. **Accountability** – Sunbeams is responsible for and able to demonstrate compliance with the above principles.

4. Legal Framework

This policy is written to ensure compliance with the following legislation:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Privacy and Electronic Communications Regulations (PECR)** – applicable only for marketing or fundraising activities.

5. Types of Data We Collect

We may collect and store the following types of personal data:

- Names, addresses, contact numbers, and email addresses
- Dates of birth
- Photographs and video footage (with consent)
- Demographic information including gender, ethnicity, religion
- Health and safeguarding-related information (where appropriate)
- Educational and employment background
- Communication records and service interaction logs
- Volunteer application and vetting details

6. Purpose and Retention of Data

Data is collected for the following purposes:

- Delivering our services to mentors, mentees, and families
- Staff and volunteer recruitment, training, and management
- Monitoring and evaluation
- Marketing and fundraising communications (only with consent)

Retention periods:

- Most personal data will be retained for **6 years** after the end of service or contract, unless legally required to retain it longer.
- Volunteer application records and DBS certificates are retained for **up to 12 months** unless the volunteer continues in service.
- Marketing consent records are retained until withdrawn.

All retention periods are reviewed annually.

7. Access to Data

Access to personal data is granted on a strict need-to-know basis:

- **Executive Director and Senior Managers**: Full access for operational oversight and safeguarding.
- **Volunteer Coordinator and Program Staff**: Access to data required for mentoring delivery, including sensitive data with appropriate safeguards.
- **Board Members**: Limited access where explicitly authorized (see "Confidentiality Policy").
- **Administrative Staff**: Access to limited contact data and service records as required.

All individuals with access are trained in data protection responsibilities.

8. Subject Access Requests (SARs)

Any individual has the right to request access to their personal data held by Sunbeams. The process is as follows:

- Requests must be submitted in writing or via email to the Executive Director.
- Identity verification will be required before release.
- Sunbeams will respond within **one calendar month** of receiving the request.
- Where requests are complex or numerous, this deadline may be extended by up to **two months**, with notification provided to the requester.

We will provide the data in a commonly used, accessible format unless another format is requested.

9. Data Destruction

Sunbeams uses the following methods to destroy data securely:

- **Paper records** are shredded using cross-cut shredders or collected by a licensed confidential waste service.
- **Electronic files** are securely deleted from systems and devices using permanent wipe software.
- **External storage devices** (e.g., USBs, CDs) are destroyed or securely wiped before disposal.

Backups are encrypted and subject to the same retention and destruction rules.

10. Confidentiality and Data Protection

All staff and volunteers are bound by confidentiality obligations and sign a confidentiality agreement upon engagement. Access to personal information is strictly controlled and discussed only where necessary and lawful. Confidentiality applies to verbal, written, and digital information.

Confidentiality, however, is not absolute. There are circumstances where information must be shared in order to protect a child, young person, or vulnerable adult from harm. If staff or volunteers believe a child or individual is at risk of abuse, neglect, or serious harm, they are legally and ethically obliged to share relevant information with the Designated Safeguarding Officer (DSO) or Deputy DSO. In such cases, the duty to safeguard and protect life takes precedence over the duty of confidentiality.

Staff must not promise absolute confidentiality to service users. Instead, they should explain that information will be kept private unless there is a safeguarding concern that requires sharing with appropriate authorities. All such decisions must be recorded in line with the Safeguarding Policy and reported immediately to the DSO.

11. Data Sharing and Transfers

Sunbeams does not sell or share personal data with third parties except where:

- Required by law (e.g. safeguarding, court orders)

- Necessary to fulfil contractual or funding obligations (with appropriate agreements)
- The data subject has given explicit consent

Data is never transferred outside the UK without additional legal safeguards.

12. Monitoring and Review

The Executive Director is responsible for the implementation and monitoring of this policy. Compliance audits and risk assessments are conducted annually. The policy is reviewed every 12 months or sooner if legislation changes.

Contact for Data Protection Issues
Executive Director
Sunbeams
97 Stamford Hill, London N16 5DN
Email: admin@sunbeamslondon.org.uk
Phone: 020 3519 8878