PRIVACY POLICY

At Survivors of Bereavement by Suicide (SoBS) we are committed to protecting your privacy. The purpose of this policy explains when and why we collect personal information about people who use our services, visit our website, contact our Helpline, join our support groups or email support. This policy explains how SoBS processes your data, whether you are using our services, interested in volunteering, making a donation or just browsing our website.

SoBS takes appropriate technical and organisational measures to keep your data safe, so we may change this policy from time to time, so please check the policy statement page on our website occasionally to ensure that you are up to date with any changes. By using our website, you are agreeing to be bound by this policy.

Any questions regarding this policy and our privacy practices should be sent by email to admin@uksobs.org or by writing to SoBS, 14 – 16 New Lawn Close, Ilkeston, Derbyshire, DE7 5HE. Alternatively, you can telephone 0115 944 1117.

SoBS supports people in need of our service through its peer led support, which is available via telephone, email, letter and face to face in a number of locations throughout the UK.

SoBS Support

Helpline

All data received through telephone contact with our Helpline Volunteers is initially noted, this will help to assist with the nature of the call and to process bereavement packs to individuals. All collated details are to be destroyed once the requested information is sent out. Helpline Volunteers need to destroy any personal details they have taken from the caller by shredding.

A record of your phone number is automatically stored on our bespoke helpline system, which is only visible to our staff in the National Office. If you wish to remain anonymous, please prefix your call with '141'. However, if you contact the National Office direct, all calls are recorded for training and legal purposes and are cleansed weekly. Only telephone numbers are stored on our central systems and can only be accessed by the National Office, unless you give your details during the call for information to be sent out to you.

If a caller gives consent and shares their details within a voicemail message the volunteer will endeavour to contact them within 24 to 48 hours. The volunteer must either withhold their number or prefix their outgoing call with '141' for safeguarding their identity. Any information taken by the volunteer must then be destroyed by shredding on completion of the call.

Volunteers must ensure their personal information is kept secure and adhere to the safeguarding policy if returning a call to a service user.

Any concerns Helpline Volunteers have regarding callers should be reported to the National Office as soon as possible giving the date and time of the call.

Calls to the Helpline regarding matters other than bereavement support need to be directed to the National Office.

Third Party Requests

We will not process any third party requests. Any information shared or processed for our services can only be posted to those requesting it, i.e. we do not post a bereavement pack on behalf of a friend or relative.

Groups

All data received through telephone, email or face to face contact will be stored by the data controller (Group Leader/volunteer). This will help to assist with the nature of the service required.

The following details which may be stored, but only with your consent, will be data cleansed after 2 years unless there is good reason to retain your data;

- Name
- Address
- Telephone number
- Email address

Information is taken initially to enable us to send a bereavement pack along with a map for the location of the venue of the meeting. Agreed consent to contact a survivor is required for a group leader or volunteer so they can make them aware of any cancellations of sessions and reminders of when sessions run, or if there are any events taking place locally which SoBS maybe involved in.

For those who loan books, details will be required to ensure the item is returned.

Those who fundraise on behalf of SoBS will have their data stored for the purpose of the event and sending a letter of thanks for donations. Any consent given by the fundraiser allows us to share the event details and limited personal data (i.e. name and geographical area) on our website, social media and newsletter.

If you make contact by telephone and wish to remain anonymous, please prefix your call with '141'. However, if you contact the National Office all calls are recorded for training and legal purposes and are cleansed weekly. Only telephone numbers are stored on our central systems and can only be accessed by the National Office, unless you give your details during the call for information to be sent out to you.

On the occasion, if it is required that a volunteer needs to return a call and the caller has shared their contact details and given consent, the volunteer must prefix their outgoing call

with ‘141’ to safeguard the volunteer’s information. Any information taken by the volunteer must then be destroyed by shredding on completion of the call.

Volunteers must ensure their personal information is kept secure and adhere to the safeguarding policy if returning a call to a service user.

Group leaders are the Data Controllers for any information collated, stored and shared and have to adhere to the same policy and procedure for data cleansing as the National Office. Link to policy required. This requires all group leaders to ensure they have written consent to continue to store your personal data for a period of 2 years and will then contact you prior to data cleansing to request an updated consent form. If further consent is not received all data will be shredded or electronically deleted. How is this followed up with volunteers.

Email

All emails are dealt with in strict confidence between the receiver and the sender and no information shared, unless concerns for the safeguarding of the individual, legal purposes and any resource requests.

All block emails need to be blind copied (bcc) to ensure individual personal email addresses are kept secure and not visible to others.

All emails are to be electronically deleted (or shredded if printed) for data cleansing every 2 years, with the exception of financial - 7 years, legal/complaints/grievance – 7 years after the date of the dispute is resolved.

National Office

- If you contact us by email, we will ask your permission to share your data with the relevant volunteer. Your actual email address may be visible in the addressee line, this depends on how your computer is set up. If you would like to avoid this, you should review the whole of your email message (including any historic messages, usually shown below your current reply) before you press send, and delete any mention of your email address.
- If you wish to access a group session and contact us by letter, then your data will be shared with the group leader or relevant volunteer.
- If you contact us by phone or face to face we will ask your permission to share your data with the relevant volunteer.
- We will not contact you via a third party sharing your information and this data will not be kept.

In general, we try to keep as little information about you as possible. Volunteers may take notes when they talk to you to assist in the conversation. These notes are shredded at the end of the call.

We also record some statistical information which is generated by our website, national Helpline and group attendance. However, this does not record any detailed personal data. This information never reports about specific people.

In certain circumstances we may have concerns about your safety, such concerns always outweigh consideration of confidentiality. Particularly if we feel there may be a threat to yourself or others. Reference to Safeguarding policy and Disclosure.

Any data held for legal, complaints or grievances will be data cleansed every 7 years after the date of the dispute is resolved.

We'll never pass any of your information on to any other organisation, except in the following situations:

- We receive a court order requiring us to share information.
- You directly ask us to pass on information about you to someone else.
- You threaten the safety of our Volunteers.
- You compromise the delivery of our service, for example by making it difficult for other people to get through, or by misusing the telephone system or other technology.

From time to time we have to take decisions to limit an individual's access to our service. If this happens, we will make every effort to inform you as to the reason why we have restricted your access.

If we believe you are abusing our service or are abusive towards Volunteers, we will use our system to block your calls or messages from getting through and restrict access to any groups. In extreme situations we may also involve the police. If you wish to appeal our decision, please contact the National Office.

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access 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 date being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal date.

A personal date breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data

breach whenever any personal data is lost, destroyed, corrupted or disclosed; If someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

If a personal data breach occurs, we will:

- Notify the ICO In full
- Record details in breach log (appendix 1)
- Investigate how the breach has occurred

The investigation will be completed by the Chief Officer and a Trustee of the Board. A report will be written of their findings and procedures amended/updated to prevent reoccurrence.

If you want to complain

SoBS aims to support all survivors over the age of 18 years to the highest possible standard at all times. To help achieve this, we encourage anyone who is not completely happy with the service they have received to let us know immediately, by contacting the Chief Officer at the National Office, by completing the complaints form.

It is important that you give as much information as possible, to enable us to fully investigate your complaint. Your information will not be passed on to anyone outside of SoBS. So we can effectively handle a complaint, in some cases we will need to involve the Chair of the Board of Trustees, in completing and signing the complaints form, you are agreeing to the Chief Officer sharing your information with the chair to resolve the complaint.

- Complete the appropriate complaints form (see Appendix 2) and post to: The Office Manager, SoBS National Office, 14 – 16 New Lawn Road, Ilkeston, Derbyshire, DE7 5HE
- Provide proof of identity including your name and postal address. If you contact the Helpline, you will be directed to the National Office.

On receipt of your complaint an acknowledgment will be sent to you within 3 working days from the Chief Officer and a full response will be sent within 21 working days. If the Board of Trustees are required to undertake any further enquiries, they will report the decision to the complainant within thirty days. The time limits expressed in this procedure will be regarded as the normal time limits. They may however be extended by mutual agreement.

Data cleansing of any complaint is undertaken every 7 years after the complaint has been resolved and all records will be shredded or removed off electronic systems.

If you would like to volunteer with SoBS

If you are interested in volunteering with SoBS, you will be asked to give us your personal details. You can apply to be a volunteer by contacting our National Office, website, post, email, or at events.

SoBS will use your information to allow us to process requests for volunteering, follow up references and assist you with any queries you might have regarding your volunteering application. By completing the application, you consent to the processing of this information by us. The information provided will be used to make a decision about whether you will be accepted or declined as a volunteer. The following information will be shared with the National Office and Board of Trustees to process your application;

- Name
- Address
- Telephone Number
- Email address
- DOB

You must also obtain consent from referees for their information to be shared, for the purpose of processing your application.

Unsuccessful applicants will be notified and all data held will be shredded or removed immediately.

Volunteers who are successful will have their application and data stored for a period of 2 years, at which time they will be contacted prior to data cleansing to ensure they are agreeable to SoBS retaining their data.

Sharing information outside of SoBS

SoBS will keep your personal information confidential, unless we are required to disclose it in connection with a police investigation and/or we have reason to believe that you may present a risk of harm to yourself or others.

We may be required to share your volunteer information to provide a reference, at your request.

If you donate to SoBS

When you donate money to SoBS or fundraise, we may collect and process information about you. This information may include your name, email address, postal address, telephone or mobile number. Some of this information may come from external sources.

By sharing your data, you will be consenting to SoBS holding information and we will take appropriate measures to ensure it is protected. We will hold your personal information on our systems for a period of 7 years, due to financial regulations for Gift Aid and HMRC. After 7 years all data will be cleansed either by shredding or electronic deletion. If you wish to setup a fundraising page, such as PayPal, Virgin Money Giving or Just Giving websites (see their separate privacy statements).

We may also use your information for a number of purposes including:

- To process donation's you have made.
- For administration purposes, including thank you letters (for example, we may contact you regarding a donation you have made or the event you have registered for).
- For internal record keeping, including the management of any feedback or complaints.
- If you have made a Gift Aid declaration, we may disclose the information you have provided as part of the declaration to HMRC for the purpose of reclaiming Gift Aid on your donation(s).

You can donate to SoBS via your mobile phone either on a one-off basis or through a monthly subscription service. We work with JustGiving to provide and administer the text-to-donate service, and calls about this service including how to opt out of calls or texts, will be routed through this supplier (see their separate privacy statement).

Using our website

Our website uses cookies, as almost all websites do, to ensure that you can interact with the website successfully and to help provide you with the best experience we can. Cookies are small text files that are placed on your computer or mobile phone when you browse websites.

Our cookies help us:

- Make our website work as you would expect
- Improve the speed/security of the site
- Allow you to share pages with social networks like Facebook
- Continuously improve our website for you
- Make our services more efficient
- Save you having to login every time you visit the site

We **do not** use cookies to:

- Collect any personally identifiable information (without your express permission)
- Collect any sensitive information (without your express permission)
- Pass data to advertising networks
- Pass personally identifiable data to third parties

If you subscribe to SoBS Communication

If you wish to sign up to our newsletter, we will require a signed consent form allowing for your data to be held, which will be reviewed every 2 years or you can unsubscribe by contacting the National Office.

In May 2018, we moved to an 'opt-in only' communication policy. This means that we will only send communication to those that have explicitly stated that they are happy for us to do so via their preferred channel(s) (email, SMS, phone or post).

Right of Subject Access

You have the right under the Data Protection Act 1998 to request for a copy of the personal data we hold about you and to have any inaccuracies in your information corrected. If you wish to make a subject access request (SAR), you will need to provide us evidence of your identity to enable us to start the process. We will acknowledge receipt of your request within 3 working days of receiving and on receipt of payment we will process within 28 working days. If the information contains details of another person or you are making a request on their behalf, they will need to provide us with written and signed authority to enable us to proceed. If we do not receive this, we will seek their consent before we provide any information to you.

FEES - Please note that there will be a charge of £10.00 to cover the administrative costs of responding to a subject access request. Unless we have indicated otherwise, please submit a cheque for £10.00 payable to SoBS with your request, otherwise we will not be able to process it.

We will ask you to:

- Complete the appropriate form (see Appendix 3) and post to: The Office Manager, SoBS National Office, 14 – 16 New Lawn Road, Ilkeston, Derbyshire, DE7 5HE
- Provide proof of identity (give examples) including your name and postal address. If you contact the Helpline, you will be directed to the National Office.
- Pay a fee of £10

We will only send a response to a subject access request to you by registered mail.

You should also note that if we are unable to verify your identity, for example if you contact the service anonymously or use a different name to do so, it will not be possible to provide you with the information requested.

If you wish to make a request for your data without completing the Subject Access Review form, this **must** be done in writing, either by email or sending a hardcopy. Please ensure you provide all the relevant information, as missing information could result in a delay to the start of the process.

All data held for SAR's will be data cleansed after 2 years, either by shredding or electronic deletion.