Survivors' Network

Data Protection Policy

Key Contact: CEO
Date Agreed: March 2021
Review Date: March 2024

Scope

Survivors' Network is committed to being fully compliant with all applicable data protection legislation and to following good practice in respect of all the personal data it holds, both in electronic form and on paper.

'Data protection legislation' includes the Data Protection Act 2018 and the UK GDPR, as modified or replaced from time to time, and any other related legislation (such as the Privacy & Electronic Communications (EC Directive) Regulation 2003).

This policy should be read alongside Survivors' Network's confidentiality policy, and any other policy or guidance relating to the handling of personal data.

1. Good practice

Survivors' Network will, at all times comply with the data protection principles and other obligations in the data protection legislation, including:

- Obtaining and using personal information only on a sound lawful basis and for a clearly defined purpose or purposes;
- Ensuring that the right information is held, enough but not too much;
- Ensuring that as far as possible the information is accurate and up to date;
- Informing individuals of how their personal data is or will be used;
- Holding personal data no longer than necessary;
- Recognising the rights individuals have over their data and responding appropriately;
- Ensuring that all personal data is held securely and access is properly authorised;

- Understanding the restrictions on transferring data outside the UK.

2. Responsibilities

Overall responsibility for implementation of this policy is delegated by the Board of Trustees to the Chief Executive Officer.

All managers are responsible for (a) ensuring that procedures within their remit are consistent with this policy and (b) monitoring compliance with relevant policies and procedures that support data protection.

All members of staff, volunteers, contractors and subcontractors are required to comply with this policy and its related procedures where applicable.

Survivors' Network undertakes to provide appropriate guidance and training, including regular refresher training, to all members of staff and others who handle personal data on its behalf.

3. Assessments

Survivors' Network will carry out a Data Protection Impact Assessment in the following situations:

- Whenever it is proposed to enter into a data sharing agreement with a new partner, or to make modifications to an existing data sharing agreement.
- Whenever a new project or activity is established that involves the processing of special category and/or criminal record personal data, or where other risks can be identified.
- Whenever an existing process involving the use of personal data is significantly modified (and in particular where it is proposed to start processing special category and/or criminal record data).
- Whenever it is proposed to share special category and/or criminal record data outside an existing data sharing agreement, unless the disclosure is an isolated case and made to an appropriate authority.

Survivors' Network will carry out a Legitimate Interests Assessment in the following situation:

- Where new processing is envisaged on the basis of legitimate interests and the situation is not substantially the same as processing for which a legitimate interests assessment has already been carried out.

In addition, an appropriate assessment will be carried out whenever an incident occurs that suggests that a risk has not previously been sufficiently evaluated.

4. Data sharing

Survivors' Network may share personal data with other organisations only in one of the following circumstances:

- Under the terms of a joint data controller agreement.
- Under the terms of a data sharing agreement.

- Under the terms of a data processor contract.
- With the explicit consent of the data subject.
- In circumstances where there is concern for the safety or wellbeing of the individual or someone else as per the Safeguarding Adults or Children's policies.
- In exceptional circumstances on the authority of the Chief Executive Officer, who shall determine the basis on which the sharing may legitimately take place.

5. Notification

Survivors' Network complies with its obligation to pay an annual fee to the Information Commissioner at the charity rate.

6. Security

Survivors' Network understands its security obligations. All users of IT systems and those who handle personal data in hard copy are required to follow the protocols and guidance set out in Data Protection Guidance for Staff

Relevant IT systems are reviewed at least every two years to ensure that they incorporate up to date security measures.

Bearing in mind that many security breaches are the result of human error rather than systems failure, all those who handle personal data on Survivors' Network's behalf receive specific training and reminders on appropriate precautions.

In the event of a data breach, potential data breach or 'near miss', the CEO or nominated person will:

- Investigate the nature and extent of the incident.
- Take immediate steps to prevent any further harm.
- Inform the Management Committee.
- Report the incident to the Information Commissioner if it reaches the required threshold.
- Inform any individuals who may be seriously adversely affected.
- Review the incident and report to the Management Committee on lessons learned.
- Implement proportionate changes to systems and procedures in order to minimise the risk of a similar breach recurring.

All those who handle personal data on Survivors' Network's behalf are placed under an obligation to report any data breach, potential data breach or 'near miss' to the CEO immediately they become aware of it. Prompt reporting is regarded as a strong mitigating factor if a breach is reported by the person responsible for its occurrence.

7. Transfers abroad

Survivors' Network avoids transferring personal data outside the UK as far as reasonably possible. Whenever a service is employed that involves processing personal data outside the UK, the data is kept within jurisdictions that have been assessed as 'adequate' where possible.

Any other transfer of personal data outside the UK must be approved in advance by the CEO who will ensure that the transfer is compliant with the UK GDPR.

8. Accountability

Survivors' Network retains records to demonstrate its compliance with the UK GDPR including:

- Evidence that consent has been obtained, where this is the basis for processing
- Training of staff and others on the data protection responsibilities
- Data Protection Impact Assessments
- Legitimate Interest Assessments
- Joint controller agreements
- Data sharing agreements
- Data processing contracts
- Data Subject Access Requests and the response
- Details of any other exercise of data subject rights and the response
- Security breaches, potential breaches and near misses, whether or not they reach the threshold for reporting to the Information Commissioner
- Security reviews

9. Children

As a provider of online services to children, Survivors' Network will:

- Ensure that information about the data protection implications is available to children in a form that they will best understand;
- Seek verifiable parental consent where the child is under the age of 13, except where consent is not required in connection with a preventive or counselling service.

10. Training

Survivors' Network must ensure that all its employees and volunteers are aware of Survivors' Network's policies and procedures and understand their personal responsibility to follow these in order to protect personal data appropriately.

Whilst the CEO has overall responsibility for data protection, she may identify a separate data protection lead within the organisation. Where this is not the CEO, this will be specified within the Data Protection guidance for staff.

Survivors' Network will provide appropriate and relevant training to all its staff and volunteers. The data protection lead or CEO will ensure that general training is provided at least once every two years or when there are significant changes to data protection legislation or Survivors' Network's policies or procedures. Managers are responsible for identifying specific training needs within their teams, and should ensure that data protection considerations are included in informal training, such as during team meetings.

The data protection lead will ensure that staff with specific data protection responsibilities have access to information on developments in this area (such as through briefings from the Information Commissioner's Office and specialists in this area) and individual training if required.

Survivors' Network will keep records of attendance at all data-protection-related training.