

Sophia Pregnancy Loss Support

Data Security Breach Policy

N.B. For the purpose of this document, Sophia Pregnancy Loss Support may also be referred to as ‘SPLS’.

**Introduction**

Sophia Pregnancy Loss Support (SPLS) collects, holds and processes personal data of individuals. We realise the importance of keeping this data safe and secure; care is taken to protect personal data from data security breaches that could compromise security. We are acutely aware that a data breach may result in harm to individuals, damage reputations and cause a detrimental effect on the service that we can provide.

As an organisation that processes personal data, Sophia Pregnancy Loss Support has a data breach security breach policy in place. This policy has been written in case the situation arises whereby there is unauthorised or unlawful processing of data, or where there is accidental loss, destruction of or damage to personal data.

A data security breach can happen for many reasons. Some of which include;

* Loss or theft of equipment on which data is stored
* Access by an unauthorised third party
* Equipment failure
* Human error
	+ Sending personal data to an unintended recipient
* Hacking
* Deception from individuals where information is obtained by misleading SPLS

This policy sets out the procedure to ensure a consistent and effective approach to managing a data breach. It applies to all trustees, members of SPLS as well as volunteers and data processors working on behalf of the charity.

**The objective of this policy is to minimise the risk associated with a security breach and to consider the necessary action needed to secure personal data to prevent further breaches.**

**Reporting a data breach**

Any individual who has access to sensitive personal data held by Sophia Pregnancy Loss Support is responsible for reporting an information security incident as soon as is practicable to our ‘Data Champion’ at Sophiagroup16@gmail.com.

Accurate details of the incident, when the breach occurred (date and time), who the data breach relates to and which information has been accessed should be given when reporting a data security breach.

**Containment and Recovery**

Once a data breach report has been received, the Data Champion will need to determine if the breach is still occurring. Appropriate steps will be taken immediately to reduce the effect of the breach, if this is the case.

The Data Champion will make an initial assessment to establish the severity of the breach and they will determine whether anything can be done to limit the damage caused by a security breach. Advice may be sought from Trustees of Sophia Pregnancy Loss Support in order to resolve the incident quickly. If appropriate, the Data Champion will inform the police as soon as possible of the security breach in an effort to ensure the safety of those individuals whose data has been impinged. A suitable course of action must be taken to resolve the incident.

**Investigation and Risk Assessment**

The Data Champion will undertake an investigation within 24 hours where possible, once a security breach has been identified or reported. This investigation will involve an assessment of the risks associated with the breach, such as, the potential consequences for individuals whose personal data has been breached, how serious they are and how likely the potential consquences are to occur.

The investigation should include;

How many individuals’ personal data has been affected; how they are associated with SPLS (e.g. trustee, volunteer, member); the type of data involved and how sensitive the information is; the protection SPLS had in place (e.g. passwords); whether the data has been lost/stolen/used for inappropriate means; whether the data could be put to illegal/inappropriate use; the individuals affected by the breach and the potential risks to them; whether there are wider consequences to the breach.

**Notification**

Informing those affected that Sophia Pregnancy Loss Support has experienced a data security breach is an important element in our breach management strategy.

The Data Champion and relevant trustees will need to establish whether the breach is significant enough to inform the Information Commissioner’s Office (ICO). If it is the case that the ICO needs to be informed, this will be informed within 72 hours of becoming aware of the breach.

Every breach should be assessed on a case by case basis. Those evaluating the breach should consider, who to inform (e.g. ICO, police), as well as the following:

 Whether the breach result in a risk of affecting the individual’s rights and freedom.

Would notification help to prevent unauthorised/unlawful use of personal data?

Would notification allow the individual affected to act to ensure their safety? They should be notified without undue delay; this should include a description of how and when the breach occurred, as well as the data affected by the breach.

 Is the advice given to those affected clear, and adapted if necessary, to ensure they are aware of what they can do to protect themselves as a result of the data breach? The guidance must also include information on the action Sophia Pregnancy Loss Support has already taken to lessen the risks associated with a data breach and should include what we are willing to do in order to help them.

Individuals should be provided with the charity email address so that they can contact SPLS for further assistance and information on what has happened.

There are a number of ways to notify those affected by a data security breach. The Data Champion should consider using the most appropriate one. They must weigh up the security of the means used to inform, as well as the urgency of the situation.

Sophia Pregnancy Loss Support will maintain a record of any data breach, regardless of whether notification was required.

**Evaluation and Review**

Once the Data Champion and relevant trustees have contained the incident, they will perform a full review of what caused the breach, how effective the response to the breach was and the changes to the policies and procedures that may need to occur to prevent further breaches.

The review should consider; where and how the personal data is held and stored; where there are weak points within our security measures; whether methods of transmission of data are secure; trustee and volunteer awareness of confidentiality and risks associated with not adhering to this.

A report may be written with recommendations for changes to systems, policies and procedures for SPLS to undertake to minimise the risk of further data security breaches.

May 2018