SIGNAL Family Support Data Protection Policy

Introduction

SIGNAL Family Support Ltd [SFS] needs to gather and use certain information about individuals (ie, the group's members).

This Policy describes how this personal data must be collected, handled and stored to meet the group's data protection standards and to comply with the law.

Why this Policy exists

This Data Protection Policy ensures that SFS:

- Complies with data protection law and follow good practice.
- Protects the rights of staff and members.
- Is open about how it stores and processes members' data.
- Protects itself from the risks of a data breach.

Data Protection Law

The Data Protection Act 1998 [DPA] describes how organisations – including SFS – must collect, handle and store personal information.

These rules apply regardless of whether the data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The DPA is underpinned by eight important principles which state that personal data must be:

1. Processed fairly and lawfully.
2. Obtained only for specific, lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up-to-date.
5. Not held for longer than necessary.
6. Processed in accordance with the rights of the data subjects (SFS members).
7. Protected in appropriate ways.
8. Not transferred outside the European Economic Area, unless that country or territory also ensure an adequate level of protection.

People, Risks and Responsibilities

1. Policy Scope

This Policy applies to all staff, sessional workers, members and volunteers involved with SFS.

It applies to all data that the group holds relating to identifiable individuals, even if that information technically falls outside the scope of the DPA.

2. Data Protection Risks

This Policy helps to protect SFS from data security risks, including:

- Breaches of confidentiality, eg, data being given out inappropriately.

- Failing to offer choice, eg, members should be free to choose how SFS uses their data.
- Reputational damage, eg, SFS would suffer if unauthorised people gained access to sensitive data.

3. Responsibilities

Everyone who works for or volunteers with SFS has some responsibility for ensuring data is collected, stored and handled appropriately.

Anyone who handles personal data must ensure it is handled, processed and stored in line with this Policy and general data protection principles.

Key areas of responsibility:

a) SFS directors/trustees are ultimately responsible for ensuring that SFS meets its legal obligations.

b) The Data Controller (currently the SFS Manager) is responsible for:
   - Keeping directors/trustees updated about data protection responsibilities, risks and issues.
   - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
   - Arranging data protection training and advice for people covered by this Policy.
   - Handling data protection questions from anyone covered by this Policy.
   - Dealing with requests from individuals to see the data SFS holds about them.
   - Checking and approving any agreements with third parties that may handle the group's sensitive data.
   - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

General Guidelines

The only people able to access data covered by this Policy should be those who need it to enable the functioning of SFS and its activities.

Data should NOT be shared informally. If access to confidential data is required, it can be requested via the Data Controller.

Everyone who handles data for the group must keep data secure by taking sensible precautions and following these guidelines.

Personal data must NOT be disclosed to unauthorised people, whether within SFS or externally.

Data should be regularly reviewed and updated if found to be out of date or inaccurate. If no longer relevant it should be deleted.

If in doubt about any aspect of data protection, seek the advice of the Data Controller.

Data Storage

On paper:

If data is stored on paper it must be kept in a secure place where unauthorised people cannot access it.

Care must be taken not to leave paper data where unauthorised people could see it.

Once it is no longer needed it must be shredded.

Electronically:
Data should be protected by password.
If stored on removable media these must be kept in a secure place when not in use.
Sensitive data should not be stored directly on mobile devices such as phones or tablets.
Once data is no longer needed it should be deleted.

Data Accuracy
The law requires SFS to take reasonable steps to ensure data is kept accurate and up-to-date.
SFS will make it easy for members to update the information SFS holds about them.
Data should be updated as soon as any inaccuracy is discovered.

Subject Access Requests
All individuals whose data is held by SFS are entitled to:

- Ask what information SFS holds about them and why
- Ask how to gain access to the information
- Be informed how to keep it up-to-date
- Be informed how the group is meeting its data protection obligations

If an individual contacts SFS about any of these points, it is called a Subject Access Request [SAR].
An SAR can be made via email to the Data Controller who will aim to provide the information within 14 days. There will be no charge.
The Data Controller will verify the identity of the person making the SAR before releasing any information.

Disclosing Data for Other Reasons
In certain circumstances SFS may be obliged to disclose personal data to law enforcement agencies. The Data Controller will ensure any such request is legitimate before disclosing any information.

Providing Information
SFS aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights.
To this end, SFS has a **Privacy Notice** setting out this information. This Notice is available on request.