



# **Safe Start Data Protection Policy**

Policy Created: January 2020

Reviewed by: Grace Speakman

Review Date: January 2021

## **C O N T E N T S**

<b>1</b>	Policy purpose
<b>2</b>	Data Protection Act (1998)
<b>3</b>	Staff Data
<b>4</b>	Child & Young Persons Data
<b>5</b>	SS responsibilities
<b>6</b>	Staff Responsibilities
<b>7</b>	Complaints procedure

# **PURPOSE**

1.1 In order to carry out its day to day operations, to meet its objectives and to comply with legal obligations Safe Start (SS) needs to keep certain information on its employees, volunteers, service users and trustees.

1.2 The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

## **2. DATA PROTECTION ACT (1998)**

2.1.1 SS is committed to ensuring any personal data will be dealt with in line with the Data Protection Act (1998). There are 8 data principles which provide the foundation of the act, which prescribe guidelines on: the information life cycle; the purpose for which data are gathered and held; and the rights of data subjects (the individual who are the subjects of the personal data held by SS).

2.2 MYL will adhere to the 8 data principles outlined by the Data Protection Act (1998) and therefore all data that SS collects will be:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure;
- not transferred outside the European Economic Area without adequate protection.

## **3. TYPES OF STAFF DATA THAT MAY BE HELD BY SS**

3.1 Various data is held on staff relating to their employment with Safe Start. This will cover all aspects of recruitment, selection and employment including\*:

- Job application forms
- Interview assessments
- References
- Probationary and annual reviews and supervisions
- Payroll information: bank details, national insurance number as well as details of any deductions from pay.
- Sick notes and medical assessments
- Details of grievance and disciplinary proceedings including current warnings, reference requests, etc.

*\*This list is not exhaustive*

## **4. TYPES OF CHILDREN/YOUNG PEOPLE'S DATA THAT MAY BE HELD BY SS**

4.1 Various data is also kept on the children and young people who utilise the facilities of Safe Start. These details are obtained by the completion of a short registration form by parents/carers or self-declarations via self-referral. All the information provided on this form is confidential and the forms are kept locked at the appropriate centre and are only available to appropriate staff.

4.2 The data on children and young people is obtained in order to allow staff to have access to contact details and medical information, which may be necessary in the case of an emergency. This data may also be used in statistical data reports used for contract compliance and/or funding applications. These reports are authorised and designed to protect an individual's discrete data.

## **5. SS RESPONSIBILITIES**

5.1 Much of the data held by SS is, by its nature, highly personal. SS recognises that it is its duty to safeguard the data by all means possible and to inform interested staff about what is kept and why, along with information on how the data can be accessed and by whom.

5.2 The data kept on staff is exclusively in relation to their employment with SS: no unrelated data will be kept. The data kept will be used purely for the purpose of administrating and managing the employment.

5.3 Adequate measures will be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that will be taken. The majority of personal data SS collates will be kept in individual personnel files, which are in turn kept within SS's central office. In order to comply with OFSTED regulations, Line Managers may also need to securely store copies of staff files onsite. There is restricted access to these files and they are kept locked.

5.4 Data will not be held for any longer than is necessary, therefore personal data will be reviewed periodically to check that it is accurate, up to date and to determine whether retention is still necessary.

5.4 Access to staff data is restricted to Management at the appropriate level, to Payroll staff for any issues specifically relating to pay and to administrative staff (in connection with file maintenance, employment correspondence etc.). Everyone managing and handling personal information will be trained to do so.

5.5 MYL will ensure personal data is not processed except for the purpose(s) for which they were obtained or for a similar purpose. If the

new purpose is very different, the data subject's consent will be obtained.

5.6 When data has been earmarked for destruction, appropriate measures will be taken to ensure that the data cannot be reconstructed and processed by a third party.

## **6. STAFF RESPONSIBILITIES**

6.1 To meet SS's responsibilities, all staff, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised.

6.2 All staff, volunteers and trustees are also responsible for:

- Checking that any information that they provide to SS in connection with their employment is accurate and up to date.
- Informing SS of any changes to information, which they have provided, i.e. changes of address.
- Informing SS of any errors or changes in staff information. SS cannot be held responsible for any such errors unless the staff member has informed SS of them.

6.3 Staff are entitled to view their own personnel files; to do so they should arrange a mutually convenient time with central office.

6.4 The unlawful obtaining or disclosure of personal data or any other breach of the Data Protection Act by staff will be treated seriously by SS, in line with its pre-existing disciplinary procedures and may lead to disciplinary action up to and including dismissal.

## **7. MAKING A COMPLAINT**

7.1 Any staff who have concerns regarding the safeguarding of personal data should inform the appropriate manager, in line with SS's complaints procedure.

7.2 SS will endeavour to answer any queries about handling personal information in a timely manner.