Just Say Data Protection Policy

1. Introduction & Background

Just Say Parent Carer Forum (PCF) is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the group collects in accordance with the General Data Protection Regulation and the UK Laws that implement it Data Protection Act 1998 & 2018 and GDPR 2018 (**Data Protection Legislation**).

The purpose of the Data Protection Legislation is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge.

This Data Protection Policy is designed to ensure that Just Say PCF complies fully with Data Protection Legislation and that personal data is fairly, lawfully and transparently processed.

2. Scope

The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and health information. For the purposes of this Policy references to personal data shall include sensitive personal data or special categories of personal data unless stated otherwise.

The format in which the information is held is in most instances not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

The Policy applies to all volunteers of the forum and third-party contractors. We also work closely with Sycamore Trust U.K. as our grant holder and are aware of their Data Protection Policy.

3. Purpose and aims of this Policy

To protect the rights and privacy of living individuals who join Just Say PCF.To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

4. Policy Statement

Just Say PCF is not registered with the Information Commissioner's Office (the **ICO**). According to the ICO registration self-assessment as a small unincorporated constituted group run by volunteers we are exempt and do not need to register.

There are six principles of good practice identified in Article 5 of the GDPR. They say the following:

1. **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose Limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage Limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. **Security:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In simple terms, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

There are restrictions on the transfer of personal data outside the EEA and information should not be transferred outside of the UK unless it meets the requirements of the Data Protection Legislation. Any such transfers require approval from the Data Protection Officer via the Quality and Compliance Helpdesk.

Partners and any third parties working with or for the Forum, and who have or may have access to personal data, will be expected to comply with the principles of this Policy. No third party may access personal data held by the group without having first entered into a third party agreement which imposes on the third party obligations no less onerous than those to which the Fourm is committed and which gives the group the right to audit compliance with the agreement.

4.1 Data Collection

The Steering Group will identify one person as the Membership lead to collect and process personal data.

Data Minimisation is important to think about prior to the collection of any personal data and we will only collect information that is absolutely necessary.

Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's health, ethnic origin or religious beliefs as well as information about criminal offences.
We will not collect information on a member's health or criminal offences but may ask for information about a child or young person's disability.

4.2 Approach

The Forum could be fined if we use or disclose information about other people without their consent or reliance on other lawful grounds. In order to help keep personal data secure, we will take particular care when using the Internet, e-mail , discussions at Steering Group and other meetings, talking on mobile or landline telephones. It is an an offence to steal or recklessly misuse personal data.

Special care must be taken with sensitive personal data (or special categories of personal data) such as information relating to race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life or genetics.

Any breach of the Data Protection Legislation or this Policy will be dealt with under the Fourm's Code of Conduct Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

4.3 Responsibilities under Data Protection Legislation

- The whole Steering Group is the Data Controller under the Data Protection Legislation.
- Everyone is responsible for developing and encouraging good information handling practices within the group.
- Compliance with the Data Protection Legislation is the responsibility of all members of the Forum who process personal data.

4.4 Individuals' Rights

Individuals have the following rights regarding data processing, and the data that is recorded about them:

1. The right to be informed about how we process their personal data
2. The right to access their personal data
3. The right to rectify their personal data
4. The right to have their personal data erased
5. The right to restrict processing
6. The right to have a copy of their personal data in a portable form
7. The right to object to direct to marketing and profiling
8. Rights in relation to automated decision making and profiling.

If we receive a request it should be discussed ASAP with one of the Co Chairs and discuused at the next available SG

Where a person requests access to their information, this is called a data subject access request or 'DSAR':

- Just Say must usually respond within one month.
- The response must be in a permanent form, unless this is not possible, or the individual agrees otherwise.
- Unintelligible terms must be explained.
- The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

4.5 Security of Data

All SG members are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the group to receive that information and has entered into a confidentiality agreement.

Data must be fully encrypted, and password protected. If data is in a paper format (such as a sign in sheet) the SG member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transferred as promptly as possible (scanned in) and the orginal shredded.

4.6 Disclosure of Data

The Forum must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All members should exercise caution when asked to disclose personal data held on another individual to a third party.

All third-party requests to provide data must be supported by appropriate paperwork and specifically authorised.

4.7 Retention & Disposal of Data

Personal data may not be retained for longer than it is required, e.g. after a member has asked to leave the forum or their young person turns 26.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Duplicate copies of personal data should not be kept as doing so increases the risk of that data being compromised. Where there is a need to have two copies of personal data for a short timeframe to complete a task one copy should be deleted as soon as it is no longer needed.

4.8 Working with third party partner organisations

As a Forum we will be working with our grant holder Sycamore Trust U.K. and may share personal data such as a mail out but this will be on a one off basis.

Sycamore Trust UK will not have access to the encrypted password secure database.

If we enter into any arrangement with professional researchers we will have a clear written agreement and will seek consent before sharing any personal information on our Just Say members.

4.9 Personal Data Breaches

If a Personal Information Breach occurs – for example, loss of a memory stick or accidental disclosure of personal data to a third party this must be reported to one of the Co Chairss and discussed at a SG meeting.

Advice can be sought from the CEO at Sycamore Trust UK or the Regional Advisor at CONTACT and where the breach is likely to result in a risk to individuals, the SG must notify the Information Commissioners Office at the soonest possible time and within 72 hours of becoming aware of the breach. Tel: 0303 123 1113 Mon-Fri 9am-4.30pm or online ico.org.uk/global/contact-us/.

If the risk of the breach is high the individuals who are affected must be informed directly and without undue delay.

4.10 Anonymisation

Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

Where personal data is collected and needs to be retained for monitoring purposes, but it no longer needs to be attributable to an individual it should be anonymised at the earliest opportunity.

Fully anonymised data can be difficult to achieve in some situations. Where this is the case it is still good practice to partially anonymise the data to lower the chance of it identifying an individual.

5. Roles and Responsibilities

5.1 Steering Group

Overall responsibility for compliance with Data Protection Legislation rests with the Just Say Forum Steering Group - everyone is responsible for making sure that the Data Protection function is fully resourced to meet the needs of the group .

5.2 Membership lead

The membership lead must act in accordance with this policy and Data Protection Legislation. They need to keep the SG - and Co Chairs- updated on any issues and raise any data breaches immediately.

Please read in conjunction with Code Of Conduct and Privacy Policy.

All Membersof the SG to sign the Data Protection Statement.

This Policy will be reviewed every two years - or sooner if the legislation changes.

Review due June 2024.