



SENDIASS Staffordshire Family Partnership

Confidentiality Policy

1. Introduction

SENDIASS Staffordshire Family Partnership (SFPS) is a statutory service offering free, impartial, advice and support to parents and carers of children and young people (CYP), (aged 0 – 25 years) and children and young people, on issues about education, health and social care relating to their CYP's special educational need or disability (SEND) (Cf. Special Educational Needs and Disability Code of Practice 2014) and to a child or young person themselves.

The information advice and support service are expected to meet Quality Standards for services providing information advice and support standards set by the IASS Network (2014).

2. Confidentiality Statement

SFPS is committed to ensuring that the confidence of parents, carers, children and young people, in its services is fostered through an explicit policy on confidentiality.

The handling of information that parents, carers, children and young people provide complies with Common Law and with the requirements of the Data Protection Act and is not shared with anyone outside of SFPS unless they have given permission for it to be shared or there are strong public interest concerns, (see Breaches of confidentiality below).

3. Definition of Confidentiality

SFPS understands confidentiality to mean that no information regarding a service user shall be given directly or indirectly to a third party which is external to the SFPS, without the service user's prior express consent to disclose such information.

SFPS may disclose information to an external party if consent is granted by a parent or carer or child and young person.

SFPS recognises that all parents, carers and children and young people should be able to access the service in confidence and that no other person should ever know that they have used them, if they wish. Information may be shared with SFPS staff whilst discussing cases; SFPS will not confirm a parent's or child and young person's use of the service without obtaining their consent. The Local Authority will not receive details of individual parents or their case.

Only SFPS staff and volunteers will have access to and respond to all correspondence/ messages/ referrals / enquiries.

4. Use of Data

SFPS maintains electronic recording systems compliant with GDPR, accessed only by staff and volunteers who have signed this confidentiality policy, to enable it to monitor take-up of the service, to identify any policy issues and provide usage statistics (in an anonymous form) to third parties. It is the responsibility of all staff to ensure that all statistical records given to third parties are produced in anonymous form, so that individuals cannot be recognised.

On occasions, the database is required to be updated to ensure efficient operation by IT staff.

SENDIASS Staffordshire Partnership (SFPS) has a paperless filing system compliant with GDPR requirements. Information is stored on a confidential database independent of the Local Authority. Service users may have access to their file at any time.

On occasion when essential, confidential information is required to be taken off site by SFPS staff and volunteers, these individuals must ensure these files are kept safe and out of sight of third parties in line with the Local Authority guidance.

Quotes from service users may be used in SFPS promotional materials in anonymous form if the service user has given prior consent for it to be used.

Photographs of parents, children and young people taken at SFPS events will only be used if written consent has been given.

5. Log Sheets

It is normal practice to ask parents and carers and children and young people for their name and address as well as other personal information relevant to them, i.e. date of birth, school, needs etc. It is the responsibility of all staff to ensure their log sheets are kept safely and out of sight of any third party, however service users have a right to be anonymous if they wish.

When information about parents or carers and children and young people is provided by a third party, i.e. other parents, practitioners and schools, SFPS staff and volunteers must confirm with the third party that they have consent to disclose such information.

6. Expressed Consent to Give Information or Make Contact

SFPS staff and volunteers must not take action on behalf of a parent or make contact with a third party without their express consent.

SFPS consider it acceptable to contact service users on their home and mobile telephones but should check with them on the acceptable method of contact. SFPS staff and volunteers should also check if it is acceptable to leave messages on answer phones and with work colleagues.

SFPS staff and volunteers will check with parents and carers and children and young people if they are happy to receive information by email. Emails will be password protected on request.

When sending information to by post, care must be taken to establish the correct mailing address, including full postcode.

Service users have the right to request that their details be removed from the database at any time.

7. Breaches of Confidentiality

SFPS recognise that exceptional circumstances may arise, in which a breach of confidentiality must be considered. These exceptions are as follows:

- Information is shared that raises concerns about a person's safety.
- Information is held by SFPS, which, if disclosed, may prevent a crime, or assist in the detection of a crime.
- Information held by SFPS which must legally be disclosed.

Circumstances in which parents, or a third party, may be at risk include the following:

- The parent discloses that they have been abused.
- The parent describes a situation which raises concerns about the safety of a child or vulnerable adult.
- The parent is in immediate danger, e.g. suicide.

Circumstances in which a child or young person, or a third party, may be at risk include the following:

- The child or young person discloses that they have been abused.
- The child or young person describes a situation which raises concerns about the safety of a child or vulnerable adult.
- The child or young person is in immediate danger, e.g. suicide.

In any of these situations SFPS staff and volunteers must consult their line manager. A decision as to whether or not to breach confidentiality should then be made.

If a decision is made to contact services for help, e.g. police, social care etc., service users should be contacted, if possible and appropriate, and informed of the decision.

If SFPS staff and volunteers receive information relating to a criminal offence, they should inform their line manager as soon as possible, who will then make a decision on whether or not to contact the police.

SFPS will disclose information where legally required to do so.

Under the Prevention of Terrorism Act 1989 it is an offence to withhold information relating to acts of terrorism. The Police and Criminal Evidence Act 1984 allows the police to make an application to a judge for a production order; it is an offence not to produce the documents referred to in the order.

In any situation where a breach of confidentiality is being considered, the situation must be recorded on the case notes as soon as possible.

8. Legislative Framework

The SFPS Advisory Group will monitor this policy regularly to ensure it meets statutory and legal requirements.

9. Ensuring the Effectiveness of the Policy

All SFPS staff and volunteers will receive a copy of the confidentiality policy. Existing and new staff and volunteers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually and amendments agreed.

This policy will be made available to parents, carers, children and young people on request.

All SFPS staff and volunteers will be required to sign the following confidentiality agreement, the original of which will be kept on their personal file.



Confidentiality Agreement for SEND Family Partnership

Name: _____

Job Title: _____

I have read and understand the SFPS Confidentiality Policy, and agree to adhere to its guidelines.

Signed: _____ Date: _____

Date of review: July 2018
Date of next review: July 2019