

POLICY AND PROCEDURE

Interagency Information Sharing

Category: staff and volunteers



SoLO
Life
Opportunities

38 Walnut Close,
Chelmsley Wood,
Birmingham,
B37 7PU

Charity No. 1102297
England Company No.
5025939

Introduction

SoLO believes that we should deliver our services in a fast, efficient and personalised manner. This clearly requires all agencies working more closely and efficiently together and to tailor the services that they provide to meet the particular needs and circumstances of each individual. Sharing information with other agencies is a key imperative to the delivery of high quality, cost effective and seamless services.

Policy Statement

The general policy and procedure defines:

- The principles which underpin the exchange of personal information between the parties who have signed up to the policy.
- The procedures which will ensure that information is disclosed in line with statutory obligations and responsibilities.
- Our own responsibility to ensure that other agencies that we share information with have appropriate policies and procedures in place.
- The purpose of the exchange of personal information; the type of information that is exchanged and the purpose for which that is used and details of other agencies that the information will be shared with.
- The roles and structures which will support the exchange of personal information between parties.
- The security procedures necessary to ensure that the confidentiality of personal information exchanged is maintained.
- How this policy will be implemented, monitored and reviewed.

Background

In the past there have been both real and perceived barriers to the sharing of personal information **for a variety of reasons including mistrust, accountability, and suitable mechanisms.**

To enable SoLO to work with other agencies; and to provide the standards of services expected by both government and the public, it is essential that these barriers are minimised. In the absence of specific statutory instruments enabling the sharing of personal information to take place, it is necessary that the organisations have a clearly defined framework to facilitate the sharing of personal information whilst respecting the rights of the individual.

This policy and procedure has been developed in accordance with *Solihull General Protocol for Inter-agency information sharing* to address these responsibilities and concerns.

Objectives

To provide a robust framework for the legal, secure and confidential sharing of personal information between SoLO and other agencies to enable us to meet both our statutory obligations and the needs and expectations of our members and volunteers.

Legal Framework

The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats eg paper, electronic, images (photograph/video) etc.

The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, it provides that if the necessary conditions of the Act can be met, sharing is perfectly legal.

The key legislation acts governing the collection and use of personal information are:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Crime and Disorder Act 1998
- Common Law Duty of Confidentiality
- Counter terrorism Act 2015
- **General Data Protection Regulations (GDPR)**

PRINCIPLES GOVERNING THE SHARING OF PERSONAL INFORMATION

General

In seeking to share personal information in order to improve services and support members and volunteers SoLO will adhere to the following principles:-

Lead person

- The organisations will appoint a lead person who will be responsible for the day to day management of the scheme within their organisation and approve individual personal information exchanges.
- The person nominated as 'Lead Person' will have sufficient seniority within the organisation to influence policies and procedures at management level.
- All Personal information exchange will be approved by the respective lead person

Personal Information Exchanges (PIE)

In order to maintain a consistent approach, SoLO will ensure that any PIE that contains the following information:-

- The full names of the organisations who are party to the PIE eg names and addresses
- The purpose(s) for the sharing of personal information.
- The type(s) of personal information that will be shared.
- Details of any other agencies/organisation to whom the personal information may also be also be shared by the recipient.
- Details of any restrictions on the use of personal information.

A specimen PIE agreement is given in Appendix A.

Confidentiality

Personal information held by SoLO shall be deemed to have been provided in confidence, in the absence of explicit or implied confirmation, when it appears reasonable to assume that the provider of the information believed that this would be the case.

SoLO accepts this duty of confidentiality and will not disclose personal information without the consent of the person concerned, unless there are statutory grounds or other overriding justification for so doing

In requesting disclosure of personal information from other organisations who have in place policies and procedures for information sharing, SoLO will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately.

Compliance with the Data Protection Act 1998

SoLO recognises its responsibilities with regard to legislation and use of personal information acquired and shall have in place appropriate policies and procedure to ensure that personal information within its care is used within the context of the relevant legislation, in particular the **General data protection regulation (GDPR) 2018**.

GDPR replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

Article 5 of the GDPR requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) 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;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) 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;
- e) 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 in so far 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
- f) 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.”

Request for Access to Records

A volunteer, worker, member (parent/carer or legal guardian), making a valid request under section 7 of the Data Protection Act 1998 for access to his/her record will be fully informed, in accordance with the Act, about the information that is held about them by SoLO.

Information that has been provided by another agency under a Personal Information Exchange Agreement may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent **must** be obtained prior to disclosure:

- The provider has specifically stated that the information supplied must be kept confidential from the member
- The information contains medical details
- The information contains information of a legal nature
- The information contains additional information about a third party

In the absence of two or more organisations having a joint (single) record on an individual, that individual may make their access to record request to any of the organisations. The organisation receiving the request will be responsible for processing the request for the whole record and not just the part that they may have contributed, subject to the conditions for disclosure mentioned above.

Consent

Unless statutory exemptions are applicable, SoLO will endeavour to seek **informed explicit consent** from the individual (or the parent/carer or legal guardian) concerned to share their personal information in accordance with the agreed Personal Information Exchange.

Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential to avoid the need to repeatedly seek consent over minor issues.

In seeking consent to disclose personal information, the individual (or their parent/carer or legal guardian) concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details, including their right to withhold or withdraw consent.

A specimen Personal Information Agreement is attached as Appendix A

For further guidance on Disclosure without Consent, see Appendix B

Time Limit on Consent

Consent to disclose personal information, obtained under a Personal Information Exchange Agreement (PIEA) will be limited to the duration of the 'piece of work'.

All agencies participating in the PIEA agree that once the 'piece of work' for which consent was originally obtained has been completed, that consent will be deemed to have lapsed.

In the event that similar or subsequent additional work needs to be undertaken with that individual, a new consent to disclose will be obtained.

Recording of Consent

SoLO in obtaining explicit consent to disclose an individual's personal information will:

- Retain the signed original consent form on the individual's manual record

All agencies participating in the PIEA will ensure that the details (including any conditions) of any consent, or refused consent, are recorded on their electronic systems in accordance with their agencies' policies and procedures.

Withdrawal of Consent/Add or Amend Restrictions

In the event that an individual:

- a) withdraws his/her consent for their personal information to be shared
- b) wishes subsequently place/amend a restriction upon the personal information that may be shared, the agency receiving such a request will immediately inform all other agencies who are or who may be affected and record the details on the individual's file

in the case of consent being withdrawn or a person applying restrictions on the use of their personal information, no further personal information should be disclosed unless there are statutory reasons for doing so, or a legal exemption can be applied.

Disclosure without Consent

Agencies who are party to the PIEA will put in place procedures to ensure that decisions to disclose personal information without legal grounds or consent have been fully considered and that such a decision can be audited and defended.

A decision to disclose personal information without the consent of the individual concerned should be authorised by a senior member of staff (nominated person) and the reason(s) recorded on the member's record.

On disclosure of the information, the agency providing the information will make the receiving agency aware that disclosure is being made without consent and the reason(s) why.

Personal information will be disclosed only where the relevant agreed purpose for sharing clearly requires this. For all other purposes, information about individual cases will be anonymous.

Making Disclosure

SoLO will ensure that staff who are authorised to make disclosure of personal information will state clearly whether the information that is being supplied is fact, opinion, or a combination of the two.

Unless it is specified to the contrary, all personal information that is provided under a PIEA will be made available to the individual should that individual make a valid request to the recipient for access to their record, under section 7 of the Data Protection Act 1988, without the necessity of seeking the provider's consent to disclose subject to the exceptions specified earlier. It is the responsibility of the staff member collecting the information to ensure that the volunteer, worker or member (their parent/carer or guardian) understands that they can ask to be consulted before information is disclosed.

Recording Disclosure

SoLO will ensure that all personal information that has been disclosed to them under a PIEA will be recorded accurately on the individual's manual or electronic record in accordance with their policies and procedures.

Procedures will be put in place to record the details of the information, and who gave and who received that information.

Disclosure of a Deceased's Personal Information

SoLO will exercise caution when contemplating the disclosure of personal information relating to a deceased person. Although the Data Protection Act

applies only to personal information of a living person, a duty of confidentiality may still apply after the person has died.

Information relating to a deceased person will be retained in a separate confidential file for a period of seven years. After this time the information retention will be reviewed.

Complaints Procedure

SoLO will operate an efficient and effective procedure to address complaints with regard to the storage and sharing of information.

In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under a PIEA, all agencies who are party to it will provide co-operation and assistance in order to resolve the complaint.

All agencies will ensure that the members will be provided with information about the complaints procedure when consent is obtained, or upon request.

Staff Confidentiality Agreement

SoLO will require staff and volunteers (full/part time; temporary; agency; students etc) who have access to, or are likely to come into contact with, personal information to sign an agreement **contained within the Information Security Policy** as part of their terms and conditions of employment or volunteer work.

Staff Awareness

SoLO will ensure that all staff are aware of, and comply with, their responsibilities and obligations with regard to:

- the confidentiality of personal information about people who are in contact with them
- the commitment of SoLO to share only information legally and within the terms of a PIEA
- information will be shared only on a need-to-know basis

Staff will be made aware that disclosure of personal information which cannot be justified, whether inadvertent or intentional, will be subject to disciplinary action.

Staff Training

SoLO will ensure that staff who need to share personal information under a PIEA are given appropriate training to enable them to share information legally, comply with any professional codes of practice and comply with their policies and procedures.

Staff and volunteers who are not directly involved with sharing personal information should not be excluded from such training as it is possible that they may come across such information during the course of their duties. It may therefore be appropriate that such staff receive awareness training.

The Staff Handbook also contains general guidelines in respect of data protection, confidentiality and information sharing.

Storage of Personal Information

SoLO has in place policies and procedures governing the secure storage of all personal information retained within manual and/or electronic systems.

Access to Personal Information

SoLO has in place policies and procedures governing the access by employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.

Retention of Personal Information

SoLO has in place policies and procedures governing the retention and destruction or records containing personal information retained within manual and/or electronic systems.

Transfer of Personal Information

SoLO has in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

- internal and external postal arrangements
- verbally, face-to-face and telephone
- electronic mail (secure network or encryption)
- electronic network transfer

Compromise of Confidentiality

Policy Name: Interagency Information Sharing
Organisation: SoLO Life Opportunities
Last Reviewed: September 2018
Next Review Date: September 2020
Version 1

Pages in this document - 12

SoLO has in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

In the event of personal information that has been shared under the PIEA having possibly been compromised, whether accidentally or intentionally, the agency making the discovery will, without delay:

- inform the information provider of the details
- take steps to investigate the cause
- if appropriate, take disciplinary action against the person(s) responsible
- take appropriate steps to avoid a repetition

On being notified that an individual's personal information has, or may have been, compromised, the original provider will assess the potential implications for the individual whose information has been compromised and, if necessary:

- notify the individual* concerned
- advise the individual* of their rights
- provide the individual* with appropriate support

(*or parent, carer or legal guardian)

Use of Personal Information other than for an agreed purpose

SoLO fulfils a number of roles. In fulfilling one particular role, staff may be given privileged access to personal information which they may subsequently believe may assist them in another role or be of wider interest to the organisation.

Personal information shared under the PIEA will have been disclosed for a specific purpose, as defined in the PIEA, and as such must be used only for that purpose.

Personal information that has been obtained under an agreed PIEA will not be regarded or used by the receiving agency as intelligence for the general use of SoLO.

SoLO staff wishing to use information for any purpose other than that defined in the PIEA, or who may wish to disclose that information to any person other than those authorised to receive it, must:

- inform the originator of the information of the intention to use the information provided for a different purpose
and

- obtain explicit consent from the individual(s) concerned or parent/carer/legal guardian before processing such information

If SoLO wishes to use information that has been provided under the PIEA for research or statistical purposes, policies and procedures are in place to guarantee that such personal information is anonymous.

Indemnity

Disclosure of personal information without consent must be justifiable on statutory grounds, or to meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both SoLO and staff member expose themselves to the risk of prosecution and liability to compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

Consent

In SoLO, consent is required for many activities. Consent can be for:

- taking part in activities
- receiving medical intervention
- photographs, social media and website
- sharing information or accessing confidential records
- **Marketing material/emails**

“How far is the person you care for able to decide for themselves?”

A child or an adult with a learning disability may **seem** unable to understand enough to consent to emergency treatment, their information being shared, or simpler issues such as photos being used in publicity etc. However, we should not assume that a person with a learning disability is not capable of consenting. It may be possible, if time is spent explaining the situation simply, for **the individual** to be able to reach an independent decision.

If an **individual** has some ability to understand and think things over, they should always be encouraged to decide themselves. This should always be the case, even when the decision is not one that either the professional or the carer will necessarily agree with. We should always strive to ask the question:

“Can the member understand and weigh up the information provided and have I done enough to assist his or her understanding?”

“What if the Member is unable to decide for themselves?”

Under English law, no-one can give consent on behalf of another adult. However, decisions can be made where the professionals can make a decision which they believe to be in the “best interests” of the member. Wherever possible, this decision will be made in consultation with the parents or carers (those with parental responsibility). People close to the person with the learning disability are often helpful in making the best decision on behalf of a person incapable of deciding for themselves. In most cases, the professional will have to make a judgement based on what is in the best interests of the member and, in all cases, where there is a dispute, more than one professional should be involved in the final decision and the discussion and decision should be documented.

Linked with the following Policies:

- Confidentiality
- Data protection
- Safeguarding
- Consent
- Information security