POLICY AND PROCEDURE

SoLO
Life
Opportunities

38 Walnut Close
Chelmsley Wood
Birmingham
B37 7PU

Charity No. 1102297
England Company No.
5025939

General Data Protection Regulations (GDPR)

Category: Staff,Volunteers and Members/Clients/Tenants

1. Introduction

SoLO Life Opportunities provides a range of high quality services to children and adults with learning disabilities which relies on up to date information being recorded and used in their delivery.

SoLO aims to ensure that all data is handled, stored and shared in full compliance with the General Data Protection Regulations (GDPR) and to ensure, at all times, the safety of our members/clients/tenants, staff and volunteers.

Data Processing that is not compliant with GDPR within SoLO Life Opportunities could present the following risks to the organisation:

- Reputation – for example, misuse of information or giving out inaccurate information that is personal to another
- Lawsuit – for example, if information on medical condition is incorrect and results in inappropriate action.
- Compensation – for loss or damage resulting from the misuse of data
- Time and effort – ineffective and inefficient systems for managing data, lost data etc.
- Distress to individuals who have been impacted on through inappropriate management of their data.

The benefits, therefore of compliance are:

- Services are developed in an effective and efficient manner and delivered to the appropriate people
- Monitoring of services is accurate and reflects the true picture
- Staff, Volunteers, Members/clients/tenants and the General Public are protected
- Up to date information is circulated to Members/clients/tenants, their parents and carers as well as those interested in our service in a timely fashion

- Staff and volunteers have the confidence to do the right thing.
- Other partner organisations have confidence in our ability to process information appropriately.

Sensitive Data

Definition under the GDPR:

Data consisting of **racial** or ethnic origin, **political** opinions, **religious** or philosophical beliefs, or **trade union membership**, genetic data, **biometric** data, data concerning health or data concerning a person's sex life or **sexual orientation**.

Other data is not considered sensitive but may be personal and should be treated as such.

2. Policy Statement

This policy is written in compliance with the GDPR
'Personal data' is information about identifiable, living individuals, held on computer or in a manual filing system.
This policy also relates to data held on mobile hand held units.
SoLO is registered with the Information Commissioner and the Data Protection Compliance Manager is the Senior Business Support Manager reporting to the CEO.

3. Key principles

- Transparency: SoLO will ensure that the Data Subject gets no surprises from the way we use their data.
- Choice: SoLO will give the Data Subject as much say as possible in the way we use their data.
- Good quality data: SoLO will endeavour to ensure that the information we hold will be accurate, up to date and appropriate.
- Security: SoLO will ensure that confidential material stays confidential and is kept safe.
- Access: SoLO will uphold the right of the Data Subject to see the data we hold and correct any mistakes.
- SoLO will only use the data kept for the purpose that is was given
- SoLO will share information with other agencies in accordance with the information sharing policy and the permission of the member, i.e. child, young person or person with parental responsibility.

4. DATA that is held within SoLO

Data will be held on the basis of the minimum required, within the legal parameters that enable us to hold it, in secure settings.

Below is an audit of information that we currently hold within the organisation, the authority under which we hold it, location and securities that are in place.

Detail	The right to hold	Where it is held	Securities
Members Profiles – including name, address, Date of Birth, ethnicity, nature of disability, Parents Name and contact details, medical conditions and medication, behavioural issues	To ensure the delivery of services is matched to need, safe and appropriate CQC requires us to hold this data Ofsted requires us to hold this data	On CRM System In Members files In key staff's homes On key staff's person (when in the community) On Project	Password protected In locked room, only accessed by authorised personnel who must sign them out and in. In locked premises, out of sight of unauthorised persons. All files will be signed in and out via the signing sheet. On the person at all times In locked boxes or bags with security padlocks On password protected tablets accessing google drive (also password protected) see appendix 5
Staff's details – including name, address, phone number, ethnicity, Date of Birth, any health conditions, NI, bank details, references, DBS	Within employment law there is a requirement to hold this data	On CRM System On SAGE system On Dovico In staff files On Project	Password protected Password protected Covered by contract In locked premises, out of sight of unauthorised persons In locked boxes or bags with security padlocks On password protected tablets accessing google

			drive (also password protected) see appendix 5
Volunteer details – including name, address, phone number, Date of Birth, ethnicity, any health conditions, references, DBS	Consent is gained to hold information To ensure that we can place volunteers appropriately and support them.	On CRM System In volunteer files On Project	Password protected In locked premises, out of sight of unauthorised persons In locked boxes or bags with security padlocks On password protected tablets accessing google drive (also password protected) see appendix 5
Funders/Supporters name, address, phone number	Consent is gained to hold information To ensure that we can connect with them and give them regular information	On CRM System In fundraising files	password protected In locked cabinet
Plan4U clients support plans	Consent to hold information To ensure that information is available when required and legitimate	Currently on the S.Drive, Migrating to Plan4U cloud system.	password protected. password protected

5. Consent

SoLO requires consent for all aspects of data handling to be implicit, clear and transparent. Consent will be recorded in appropriate ways and held centrally to ensure that people's directives are respected and adhered to. Consent can be given verbally, via email or in writing but must always be recorded.

The following describes the data held and the consent mechanisms employed with the organisation:

Data processes	Who affected	How consent is gained	Where it is recorded
Use of Photos – for internal purposes, Marketing, Social Media, Website	Members/Clients/Tenants or their representatives Staff/Volunteers	Signed form Signed form	Within the individual records CRM System As above
Permission to share information with Other Agencies	Members/Clients/Tenants or their representatives	Signed form	Within the individual records CRM System
Permission to send information about events, fundraising requests, opportunities for employment	Members/Clients/Tenants or their representatives Staff/Volunteers/funders and supporters	Signed form or emailed consent Signed form or emailed consent	Within the individual records CRM System As above

6. Right to be informed and Privacy Notices

SoLO wishes to be transparent and provide accessible information to individuals about how the organisation will use their personal data. The purpose of this is to build trust and confidence in those who access our services, whether there are staff, volunteers, members, clients or tenants or their representatives.

Privacy notices will include:

How the information will be used
What we will do with the information
Where we will share the information
How we will share the information

Privacy notices will precede the request to consent, will be written in clear, concise language using a clear font and style. Consent will be clearly stated.

7. The right for an individual to access their own data

SoLO recognises that personal data on any individual belongs to that individual and they have a right to access this data.

Information, when requested, will be provided without delay and, at the latest, within one month of receipt of the request for access. (where requests are complex and numerous, SoLO reserves the right to extend this period by a further two months and will notify the individual within the first month of this extension).

Where requests for data are manifestly unfounded or excessive, SoLO reserves the right to apply a reasonable charge for the time taken to collate information or, in extreme cases, will refuse to respond to a request. Where this action is taken, SoLO will inform the individual that this request is being refused and inform them of their right to complain to the supervisory authority for a judicial remedy within one month.

Any individual requesting information will be required to verify their identity using 'reasonable means'.

Any reference to third parties in the information will be removed to ensure their data is protected.

If a request is received for access to information under the Freedom of Information Act the matter should be referred to the Data Controller. Although SoLO as a charity and limited company is not subject to the Freedom of Information Act, it is good practice, where possible, to be transparent and open with our stakeholders. In deciding whether there is a duty to disclose the information requested, the Data Controller should consider the individual's rights of protection under the Data Protection Act and determine if the request for information is proportional. SoLO reserves the right to request qualified, professional support if there is any question about what information to release and what to withhold, or if the consequences of release may be adverse for the organisation.

Those with parental responsibility do not have a right to see their children's records unless they exercise their right to act on their children's behalf. A member of staff may need to make a judgement about a person who is acting on behalf of another. This may need to be an organisational judgement rather than an individual judgement.

Those acting on behalf of someone who is deemed to not have mental capacity and requesting personal data must be able to evidence their right to do so, this evidence, in most cases, will be Deputyship which is gained through the Court of Protection. Appointeeship, which is also a legal position, can only give authority over financial matters.

In all cases the best interest of the child/young person/vulnerable will be the deciding factor in who is able to access data.

8. Data Quality

SoLO recognises that it is in the best interests of the individual for their data to be accurate and up to date. SoLO will ensure that every effort is made to keep data

current and accurate, but recognises that the individual has a responsibility to notify SoLO of any relevant changes when they occur.

The following charts SoLO's intentions to ensuring data is constantly updated and correct.

Detail	Method of re-validation	Timescale	Control mechanisms	exceptions
Members Profiles – including name, address, Date of Birth, ethnicity, nature of disability, Parents Name and contact details, medical conditions and medication, behavioural issues	Profiles will be re-issued for signature	Annually or before accessing a new programme/home (whichever is earlier) When a change is notified or recognised that requires data to be refreshed	Access to the programme/ home will be restricted on the basis of a risk assessment.	Adults who attend drop-in schemes will be requested to update records, but not obliged to do so.
Staff's details – including name, address, phone number, ethnicity, Date of Birth, any health conditions, NI, bank details, references, DBS	Update with P60's	Annually to coincide with the end of year or in response to notification of a change DBS every three years	Employment is dependant on staff providing up to date information.	There are no exceptions
Volunteer details – including name, address, phone number, Date of Birth, ethnicity, any health conditions, references, DBS	Emailed request	Annually or in response to notification of a change DBS – every three years (or after a period of inactivity within SoLO)	Placement is dependant on Volunteers providing DBS updates	DBS will not be required in the case of supported volunteers who will be under supervision.
Funders/Supporters name, address, phone number	Emailed request	Annually or in response to notification of a change	Consent not updated will result in taken off circulation list	There are no exceptions.

9. Storage of Data

Where Data is physically stored is listed in point 4 of this policy.

9.1 Storage of data off-site (not on SoLO's premises)

There is an expectation, from the organisation that all sensitive data in staff's possession is stored for a lawful reason (e.g they have a right to the information to enable them to provide a safe and appropriate service to our members/clients/tenants). There is an expectation that, when data is stored offsite that it will be kept away from public view, where possible in a locked cabinet, box or room. If staff are unable to guarantee security at any time (e.g. they live in shared premises), they must speak to their Line Manager and determine how any risks can be mitigated against.

Where projects require data for the delivery of services to members in other community buildings (schools etc) it is an expectation that the Project Leader will ensure that the data is secured safely, away from public view and only shared with those who need to know the information. Where possible and practicable, a locked box will be provided.

Where projects are offsite for an external visit (e.g. an activity park) there is an expectation that Staff will keep personal data on their person at all times and ensure that it is locked away, out of public view wherever practicable.

Hand held devices such as IPADS, mobile phones, laptops or tablets when used to receive or hold sensitive data in relation to SoLO's work (whether SoLO equipment or personal equipment) must be password protected and data should only be stored for as long as necessary.

As identified in our staff conduct policy, staff are not authorised to take photos of any members on their own mobile phones or cameras. Where this is necessary, SoLO will provide the equipment to do this and any images will be checked for consent and stored on a central system under password protection.

9.2 Storage of data on-site (on SoLO's premises)

Where data is stored on SoLO's premises, it will be kept in a secure place where it is not accessible to anyone who does not have a right to access it.

Information stored on computers will be password protected and passwords will not be shared.
(the only exception to this would be if information was needed to be accessed to ensure the health and safety of our members/clients/tenants. After any such exception, password will be changed immediately).

9.3 Storage of data in supported living sites

It is recognised that the supported living site is a tenant's own home. The only authorised place for personal data for the use of SoLO's staff to ensure that the tenants are safe and supported, is the staff room. This data will be kept in a locked cabinet at all times.

There may be some exceptions to this when the health and safety of the tenant requires information to be displayed, for instance, dietary requirements displayed in the kitchen area. Wherever possible, the dignity of the tenant will be paramount.

9.4 Archived Data

Data will only be kept in accordance with the GDPR requirements, legal obligations and insurance requirements. All archived data will be stored in areas that are secure and not able to be accessed by any unauthorised person.

10. Disposal of Data

All data will be disposed of within the timeframe that is determined by the Legal Framework relating to its use. Data will only be kept when it is necessary for SoLO to meet its legal obligations and to ensure the health and safety of its staff, volunteers, members/clients/tenants.
Below is the timeframe that SoLO will apply to the disposal of data:

Data	Timeframe	Legal framework	Other rationale
The records of unsuccessful job applicants	6 months	Employment Tribunal	Unsuccessful candidates have 3 months (and in some cases 6 months) to file a discrimination claim
Staff who have left the organisation	7 years	HMRC Companies House	
The records of unsuccessful volunteers	Not kept	There is no legal requirement for us to keep their records	We do not have any obligation to keep these are there is no resource if we decide not to appoint
Volunteers who have left the organisation	for as long as they wish to have information	There is no legal requirement for us to keep their records	We would continue to keep their records and communicate with them until they ask us not to.
Member records after they have left	7 years	Safeguarding	We would have a 'legitimate' interest in keeping the records to be able to respond to any historic claims

Member records after they have died	7 years	Safeguarding	Although GDPR does not cover people who have died, we would have a 'legitimate' interest in keeping the records to be able to respond to any historic claims
Member contact details	Until they notify us they do not wish to be contacted	safeguarding	
Records relating to complaints or abuse	25 years	safeguarding	Files be kept until the child becomes 24 (i.e reaches the age of 18 and then allow for six years to pass, which is the period of time in which any civil claim can be brought for say negligence or vicarious liability
Incident reports/medical records	4 years	Health and Safety Executive	Accidents and incidents can only be considered within 3 years of them happening.
Funders/supporters	Until they notify us they do not wish to be contacted		

Archived data will be reviewed on an annual basis and any that no longer has a legal or insurance basis to be stored will be shredded.
Computer systems will be reviewed on an annual basis and any data no longer legally required to be kept will be removed.
Any computers that are no longer required for use within SoLO will have their hard drives removed and destroyed professionally to ensure that data cannot be retrieved unlawfully.

11. The right to erasure

The right to erasure is also known as the 'right to be forgotten'. The broad principle underpinning this right is to enable the individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The circumstances under where SoLO will erase data from their records are:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

- When the individual withdraws consent.

- When the individual objects and there is no overriding legitimate interest for continuing the processing.
- When the personal data was unlawfully processed (ie otherwise in breach of the GDPR)
- When the personal data has to be erased in order to comply with a legal obligation.
- When the personal data is processed in relation to the offer of information services to a child.

This right is not limited to processes that cause unwarranted and substantial damage or distress, although it is recognised that where this is the case, the case for erasure is stronger.
SoLO can refuse to comply with a request for erasure in the following circumstances: Where the personal data is processed for

- Exercising the right of freedom of expression and information
- Complying with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims.

In the case of children and, in particular, information shared on social networking sites and internet forums, there will be special attention paid when requests are made to remove data as the child may not be aware of the risks involved in the processing at the time of consent.

12. The right to restrict processing

SoLO recognises that there will be occasions when an individual will evoke their right to restrict the processing of data that is held about them.
SoLO will restrict the data processing in the following circumstances:

- Where the accuracy of the data is in question – all processing will be restricted until there is an assurance that the data is correct.
- Where an individual has requested restriction or erasure and the organisation is considering the legal basis under which it retains the information.

- Where SoLO determines that the processing of the information is unlawful but the individual opposes its erasure – all processing will be restricted until the legal basis is determined.

- If SoLO no longer requires the personal data but the individual requires it to establish, exercise or defend a legal claim.

When a restriction for processing data has been lifted the individual will be informed and the legal basis under which it is done communicated.

13. The right to portability

Whilst SoLO does not operate automated systems of personal data for the purpose of transferring to another provider, there is no consideration for this. However, if a time comes that SoLO does operate these systems, the organisation would comply with the regulations pertaining to this.

14. The right to object

All people that SoLO holds data on; staff, volunteers, members/clients/tenants, funders/supporters will be informed of their legal right to object against the processing of data within SoLO at the first point of contact with the organisation and this information will be contained within the privacy notice on each data collection form.
SoLO's response to objections about data processing will be:

- In the case of personal data being used for direct marketing purposes – an immediate stop to data being used.

- In the case where SoLO can demonstrate compelling legitimate grounds for the processing where the interests, rights and freedoms of the individual are over ridden or the processing of the data is for the establishment, exercise of defence of legal claims – the individual will be communicated to and any legal restriction will be applied.

In all cases, individuals objecting must have grounds relating to his or her particular situation.

15. Sharing Data

In the course of SoLO's work, there will be data sharing between agencies, such as social services, health, education and other organisations. This data sharing is to ensure that the member can access the most appropriate service with the appropriate amount of support.
Sharing of personal data needs to have a legitimate base to do so and SoLO will ensure:

- that the Data Subject knows who we are, and why and how the data will be used.

- That consent is gained and recorded from the Data Subject or their legal representative to use their data, particularly if it is 'sensitive' – covering the Data Subject's racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sex life or criminal record. This will be at the point of gathering information, recorded on individual record and on the central database.

- That the basis for sharing data is open and transparent.

Where there is a legal requirement to share data that overrides GDPR, eg. Criminal law, safeguarding SoLO will working within the legal parameters

- Data Protection is not breached if the requesting agency has a legal right to demand it.
- Data Protection is not breached if we choose to disclose information because not doing so would prejudice child protection, crime prevention, catching criminals or collecting taxes or duties.

At all times SoLO will work within the best interests of the individual.

16. Marketing

Marketing is defined as unsolicited 'communication by whatever means (of advertising or marketing material) directed to the Data Subject'
SoLO occasionally markets its services by the production of a newsletter and also the promotion of is
SoLO will adhere to the following principles:

- We will not mail out to those people who have not given consent to receive it
- We will adhere to the Telephone Preference Service check mandatory for calls to domestic lines, unless subscriber has opted in
- We will adhere to Fax Preference Service check mandatory for faxes to business lines (domestic lines only with prior consent)
- E-mail/SMS restrictions to private individuals; existing customers must be given notice and give consent (and messages must be readily identified as marketing); cold lists will not be used without the prior consent of the individual
- Web site marketing to e-commerce regulations (including information to the individual and cooling off period)

17. Automated Decision Making and Profiling

Due to the person centred approach that is taken throughout the whole organisation, there are no systems in place for automated decision making and profiling.

Should any system be identified as falling within this area, appropriate steps will be taken to ensure compliance with GDPR requirements.

18. Training

All staff and volunteers will be given training in GDPR as part of their induction and expected to comply with the principles and guidelines. Training on confidentiality will also be given to support a compliant approach to data handling.
Appendix 2 shows a flowchart of information that comes into the organisation and out of the organisation and indicates levels of authority in handling that information.

19. Compliance with data protection

To ensure that the organisation is compliant with all aspects governed under GDPR the following systems are in place:

- Data Protection Impact Assessments (appendix 4) will be carried out wherever new schemes are designed or new systems implemented. These will be stored on the shared drive and inform any changes to the current systems in place.

- The Internal Controls Audit includes Information handling whereby a Trustee will carry out an internal controls visit and interrogate the systems to ensure compliance

- Any breaches of data protection, whilst these will be avoided wherever possible, will be used as learning tools for the organisation to improve systems.

20. Breaches of data protection

Any breach of data protection will be taken very seriously by the organisation and will result in disciplinary action taken in respect of the individual held responsible.
Breaches will be communicated to:

1. The Chair of Trustees and the Safeguarding Trustee
2. The Information Commissioner
3. The Police – where the breach is considered unlawful
4. The individual who's data has been compromised
5. CQC – for those services that are under this registration
6. Ofsted – for those services that are under this registration
7. The Local Authority safeguarding board.

Each breach will be considered, on an individual basis as follows:

- The level of risk that the breach has posed to the individual
- The learning for the individual who has caused the breach
- The systems that have failed that have led to the breach

21. Management of Risk

Where there are potential risks to the organisation in relation to data protection, these will be identified and, where significant, entered onto the corporate risk register with the associated mitigating controls. The actions against the risk will be monitored by the Trustee Board to ensure that they are being managed appropriately.
The Trustee board have ultimate responsibility for the governance of risk within the organisation including the management of data.

22. Processing data internationally

SoLO does not process data internationally, but will be mindful of GDPR requirements if the situation arises that this becomes a consideration, and will put in place appropriate measures.

Links to other policies

Our organisation has the following policies that link to Data Protection, or that take Data Protection into account:

- Information Sharing
- Storage and handling of disclosure information
- DBS Policy
- Confidentiality policy
- Safeguarding and Protection of Vulnerable Adults policies
- Information security policy
- Record keeping
- Staff Conduct

Appendix 1

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

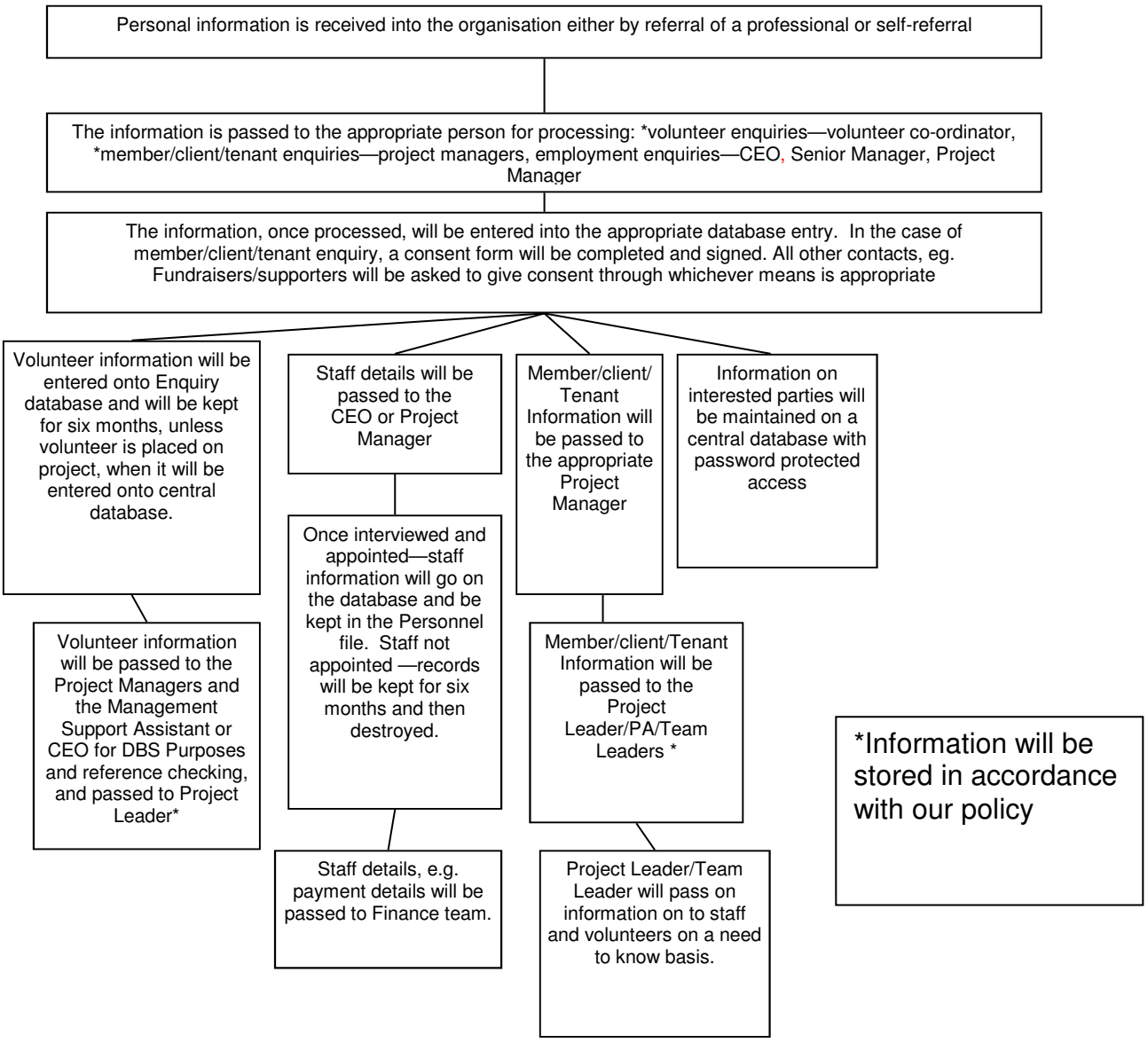
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

Appendix 2

DATA FLOW
the process



Personal information on any member/client/tenant, staff member, volunteer, or other parties that SoLO holds personal information on will not be passed to any other person outside of the organisation, unless the member of staff has authority to do so. This, however, is over-ridden if there is a serious urgent risk to the health and safety of an individual if information is not passed on. Wherever possible concerns should be referred back to the CEO.

Appendix 3

CONSENT

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

- Taking part in activities
- Receiving medical intervention
- Having photographs taken
- Sharing information or accessing confidential records

"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 (either carers or professionals) 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 member/client/tenant to able to reach an independent decision.
If a member/client/tenant 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 agree with. We should always strive to ask the question *"Can the person understand and weigh up the information provided and have I done enough to assist his or her understanding?"*

"What if the member is totally unable to decide for themselves?"

Under English law, no-one (even husbands, wives, partners, close relatives or carers) 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 service user's 'best interests'. Wherever possible, this decision will be made in consultation with the parents or carers (those with parental responsibility). People close to the person with learning disability are often helpful in making the best decision on behalf of a person incapable for deciding for themselves.
In most cases, the professional will have to make a judgement based on what is in the best interests of the person 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.

Appendix 4

Data Protection Impact Assessment

This impact assessment must be carried out when SoLO is

- Introducing new technologies and these could potentially result in a high risk to the rights and freedoms of individuals. (e.g. the introduction of a new CRM system that engages with different cohorts of individuals)

- Engaged in systematic and extensive processing activities where decisions will have legal effects (e.g. the introduction of new systems for engaging with funders, supporters etc.)

- Large scale processing of special categories of data (collating information on certain sections of our membership – e.g. those with specific disabilities)

- Introducing large scale, systematic monitoring of public areas (e.g. CCTV)

The DPIA must contain the following information:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.

- An assessment of the necessity and proportionality of the processing in relation to the purpose.

- An assessment of the risks to individuals.

- The measures in place to address risk, including security and to demonstrate that you comply

- A DPIA can address more than one project.

Senior Managers will be the authorised personnel to sign off the DPIA

Appendix 5 – Protocols relating to access to Google Drive Documents

For the purposes of keeping members safe whilst on project or out and about in the community, there will be a requirement for staff to have access to profiles which will be held for the period of the project of Google Drive. This is an encrypted site which is only accessible on approved devices with a user name and passwords. Passwords are changed after each project duration.

Only authorised staff are able to access the google Drive with the approved user name and password. This user name and password must **never** be given to any unauthorised person and doing so will evoke disciplinary action which could result in dismissal.

Approved devices, which could be a laptop, tablet or SoLO Phone must be kept password protected and secure when on project. When travelling to and from project they must be stored out of sight for the minimal amount of time possible and when stored offsite they must be put in a secure location.

Profiles and other appropriate documentation will be downloaded, from the office, to the Google Drive Platform which will be set up with a gmail account under the name of the project manager responsible for the programmes. This will be given a password. Each project will have its own Google Drive Platform and will be named accordingly.

A master excel spreadsheet, password protected, will be setup to record the gmail accounts and the passwords to ensure that when the member of staff leaves, the drive is still available.

Data will only be downloaded onto the Platforms whilst the project is active and as soon as the project is finished, all data will be removed ready for a new scheme to start. This will ensure that all data is up to date at the point of delivery.

Project Staff will be expected to record attendance using the google drive at the end of each session.