Solihull Action through Advocacy

Policy: Confidentiality and Data Protection

Date of Review: December 2020

Date of Next Review: December 2021

Solihull Action through Advocacy

POLICY AND PROCEDURE

Policy Statement

Solihull Action through Advocacy (SAtA) recognises that all individuals who use its services have a right to expect that the information we hold about them will be held in confidence and only be used for the purposes for which it was given. Not only is this a legal requirement but as a provider of independent advocacy, we believe that confidentiality and trust are at the heart of all that we do and underpin the relationship between an advocate and their advocacy partner.

As such, SAtA is committed to ensuring that personal information that is shared with or disclosed to a member of staff or volunteer of the charity is kept securely and that access to that information is controlled with the utmost care and in line with Data Protection legislation including the General Data Protection Regulation (GDPR).

The principles of confidentiality are integrated into all aspects of SAtA's work and this policy details the procedures that will be followed in order to protect confidentiality and the circumstances in which confidentiality may be breached.

Principles of Confidentiality

1. All service users have a right to dignity and respect for their privacy;
2. Service users should be able to decide if, how and when information about them may be shared with others (except in cases where the conditions for breaching confidentiality are met);
3. Information that is given in confidence should only be used for the purpose for which it was given;
4. Service users should be informed of this policy (and provided with a copy if requested) and their right for information about them to be kept confidential;
5. This policy should be available (and explained if appropriate) to other relevant agencies and individuals to ensure that all those we work with treat confidentiality with the same level of care as SAtA does.

General Confidentiality Procedures and Standards of Conduct

Sharing of Information within SAtA

Confidentiality is between the service user and SAtA and not between the service user and individual members of staff or volunteers. However, information about a service user should be shared within SAtA only on a "need to know" basis.

In general, this means that information should be kept confidential to the advocate that is working with the service user as well as the advocate's line manager. In certain circumstances it may be necessary to share that information with another senior member of staff or with another advocate (for example to provide continuity of service during a period of staff absence). The decision whether information should be shared within the organisation should always refer to whether there is a "need to know".

Staff and volunteers should be particularly careful about holding conversations about service users in open/communal areas, even if the name of the service user is not used. The dignity and privacy of service users is paramount.

Written Information

Care should be taken to ensure that written notes are accurate and respectful. Staff and volunteers should remember that service users have a right to read what is written about them. Whilst in use, written materials should not be left anywhere that they could be read by someone else and when not in use should be stored in line with the Data Protection guidance set out below.

Social Media

Staff and volunteers should take particular note that any interaction with or about service users on social media is strictly forbidden. The *Social Media Policy* provides additional guidance on this.

Sharing of Information externally to SAtA

Information will only be shared externally to SAtA with the express informed consent of the service user (or in appropriate circumstances their parent/guardian) unless the conditions for breaching confidentiality are met. These conditions are contained in this policy and are also included in the Advocates Handbook. All staff should ensure that they are familiar with the conditions and the associated procedures.

Third Party "Contractors"

When using third parties (such as interpreters for example) care should be taken to ensure that the third party either has its own confidentiality policy (a copy of which SAtA has received and considers satisfactory) or signs a confidentiality agreement to confirm that they have read and accept SAtA's policy. Where a third party is

considered to be a Data Processor under the GDPR, SAtA will ensure that a written contract is in place with that third party.

Breaching Confidentiality

Confidentiality may only be breached in the following circumstances:

1. Where the client has specifically consented to the breach.

2. Where the breach is necessary to protect the client or another person who, as a result of something the client has disclosed, the advocate believes to be at risk of harm or abuse. The *Safeguarding Adults* and *Safeguarding Children and Young People* policies should be consulted for further guidance.

3. If the advocate, despite having made every effort to do so, is unable to interpret the client's method of communication and is therefore unable to elicit their views about the potential breach and the disclosure is judged to be in the best interests of the client.

4. Where there is a legal obligation to breach (for example a court order).

5. Where the client lacks capacity to give or withhold consent for confidential information to be disclosed (in accordance with the Mental Capacity Act 2005) and the disclosure is judged to be in the best interests of the client.

6. Where the client discloses information that, if not disclosed externally, might lead to SAtA or one of its advocates assisting in a serious criminal offence. (See section of Criminal Offences below).

7. Any situation in which a client disclosed information relating to a potential Terrorism or Drug Trafficking offence.

When confidentiality has to be breached without consent, unless it is unsafe to do so the advocate will inform the client at the earliest opportunity about the reason(s) for the breach and give them an opportunity to discuss the situation and plan for the likely outcomes of the breach. Every effort should be made to ensure that the client retains as much control as possible over the process of breaching confidentiality and to keep them informed at every stage.

Any breach of confidentiality must be authorised by manager of SAtA unless there are exceptional circumstances where there is an emergency and the advocate is unable to contact a manager through the Escalation Procedure. Where such exceptional circumstances arise, the advocate must report the breach and the reason for not seeking authorisation as soon as possible to a manager.

Procedure for Breaching Confidentiality and Escalation

If the potential breach is in relation to a Safeguarding concern, the advocate should follow the procedure contained in the *Safeguarding Adults* or *Safeguarding Children and young people* policies.

Where the potential breach does not relate to a safeguarding concern:

1. The advocate should first raise the matter with their advocacy partner to explain that they may be required to breach confidentiality and to gain their views.

2. The advocate should raise the matter their immediate line manager. Line managers are responsible for ensuring that their reportees have methods for contacting them both during and outside of normal office hours.

3. If the immediate line manager is unavailable or uncontactable, the advocate should raise the matter with another manager. Contact detail for all managers are held by the administrator.

4. If no managers are contactable, the advocate should raise the matter directly with the Chief Executive Officer (CEO) whose contact information is held by the administrator.

5. The relevant manager will then discuss the matter with the advocate and make a decision regarding whether or not the information should be shared externally. This may necessitate a discussion between the manager and his/her colleagues including the CEO. The decision will take into account the nature of the information, the reasons for the potential breach and the views of the client.

6. In the event that it is decided to breach confidentiality and share information without consent, the disclosure of the information should take account of the principles of Data Protection (see below). In particular, care should be taken only to disclose information that is relevant and necessary to the purpose for which the breach has been authorised.

7. The fact of the breach, the circumstances and the decision-making process should be recorded in the client's case notes.

8. The CEO should report the breach at the next meeting of the Board of Trustees.

Criminal Offences

Because of their own vulnerability, some adults, children and young people are more at risk of abuse of all kinds, including being easily persuaded to take part in activities that may not be legal, and there will be times when they may want to discuss this activity with their advocate. This could include any crime, for example theft, burglary, benefits fraud, involvement in the supply and/or taking of drugs, and/or anti-social behaviour.

This may cause a dilemma for an advocate as to when a crime should be reported. Whilst there is no general requirement of English Law for an individual to disclose a crime to the Police, **no SAtA advocate should knowingly assist or support a client to commit an offence of any kind**.

When an advocate or other staff member is aware that an individual using the service may be/have been involved in a criminal offence, consideration will need to be given as to whether the organisation would be assisting or complicit in the offence by withholding information from the appropriate authorities.

In such circumstances the manager, in consultation with the CEO, will consider whether SAtA is likely to be at risk of prosecution or of receiving a court order to disclose known information. Such decisions will be made on a case-by-case basis.

Even if a decision is made **not** to disclose, the advocate should explain to the client the implications and potential consequences of their actions and should ensure that the client understands that, if the advocate were to be questioned by the Police or required to give evidence in court, any information they share would have to be disclosed at that time.

There are some specific circumstances that demand breach of confidentiality:

Terrorism Act 2000 and the **Anti-Terrorism, Crime and Security Act 2001**
It is a criminal offence not to disclose information where it is suspected that a person has committed a terrorist act or where that information could be of material assistance in preventing an act of terrorism.

Drug Trafficking Act 1994
It is a criminal offence not to report a suspicion or knowledge of drug money laundering.

Data Protection Statement and Principles

SAtA is committed to good practice in relation to the collecting, processing, storage and sharing of any personal data including (but not exclusively) that which relates to our service users, staff, volunteers, trustees, supporters and donors and we aim to ensure that we fully meet our obligations to comply with Data Protection legislation including the GDPR.

Moreover, SAtA recognises the benefits of good Data Protection practice over and above the need to comply with legal requirements, particularly in respect of inspiring confidence among our service users that their data will be handled appropriately and in a manner that they would expect.

SAtA is registered with the Information Commissioner (Z2309056) and the following sections detail our policy and procedures in respect of meeting those obligations.

Key Definitions

“Personal Data” is any information relating to a person who can be directly or indirectly identified by reference to that information. This is a wide definition and can include clearly personal information such as names, addresses and dates of birth but may also include other information such as reference numbers (for example National Insurance numbers).

“Special Category Data” is information that is considered to be more sensitive and therefore deserving of greater protection. This includes information such as ethic origin, political or religious views and sexual orientation.

“Data Subject” is an identifiable person to whom particular data relates.

Principles

In considering our data processing activities, SAtA is committed to the 6 principles of Data Protection as detailed in Article 5 of the GDPR.

1. **Processed lawfully, fairly and in a transparent manner**
   We will ensure that all processing has a valid lawful basis and moreover that these bases are clearly communicated to those whose data we process. We are committed to ensuring that no Data Subject will be surprised by the way that we use their data and we will take particular care to communicate what we do in an appropriate manner. We also ensure that Data Subjects know how to access their own data and that the data will be made available to them in appropriate formats.

2. **Collected for specified, explicit and legitimate purposes**
   We will tell the Data Subject when we collect data from him/her, what we are collecting, why we are collecting it and what we use it for. We will not use that data for any other purposes that are not compatible with the original purpose.

3. **Adequate, relevant and limited to what is necessary**
   We will only process the data that we need in order to carry out the purpose for which we collected it. We will not store or process any information that is not necessary to achieve that purpose.

4. **Accurate and kept up-to-date**
   We will do everything we can to ensure that the information we hold is updated and we will take swift action to correct or erase any information that is out-of-date or inaccurate.

5. **Not kept for longer than is necessary**
   We will identify data that is no longer needed and either erase it or amend it so that it is stored in way that no longer allows for the identification of the Data Subject.

6. **Processed in a manner that ensures appropriate security**
   We will ensure that we have implemented sufficient technical and organisational measures to protect the data that we hold and to prevent unlawful processing, theft or accidental loss or damage.

Data Protection Officer

SAtA has a designated Data Protection Officer (DPO) who takes a lead role in ensuring compliance with data protection for the organisation. The CEO is SAtA's DPO.

Data held by SAtA

In the course of our activities, SAtA collects and processes a variety of data belonging to a variety of Data Subjects and the table below details the types of data that we collect about different data subjects, what we use it for, where we hold it and the measure that we take to ensure that the data is safe and secure. This information may change from time to time and the most up-to-date information will always be found in our Privacy Notices (see below).

Who	What	Why	Where
Service Users	● Name ● Date of Birth ● Address and Contact Information ● Health and Disability Information ● Gender ● Ethnicity ● Sexual Orientation ● Religious Beliefs ● Communication Needs ● Risks and Safeguarding ● Mental Capacity ● Employment Status ● Relationships to others	● We need this information in order to ensure that we can deliver an effective service to the individuals whose data we collect. We cannot advocate for an individual if we do not know some or all of this information about them. ● We need to retain documentary evidence about the services and support we have provided ● We want to monitor who is using our services to make sure that we are inclusive of all those who might need our support.	● Encrypted CRM database ● Paper-based service user files stored in locked filing cabinets on SAtA premises only ● On staff/ volunteers persons when visiting service users in the community
Staff	● Name ● Date of Birth ● Address and Contact Information ● Emergency Contacts ● Nationality ● Ethnicity ● Driving Licence ● Car Registration ● Health and Disability Information ● Gender ● Sexual Orientation ● Religious Beliefs ● Marital Status ● Absence Information ● Bank Details ● National Insurance Number ● Pension Details ● Tax Details ● Student Loan Details	● Most of this information is needed to enable us to manage the employment of the data subject including issuing terms and conditions, arranging payment and ensuring we can meet social security and health and safety requirements ● We process some of this data to monitor our staff demographics to ensure our staff team is reflective of the service users we are supporting	● Encrypted HR Management Database ● Paper-based employee files stored in locked filing cabinets on SAtA premises only ● On “QuickBooks” accounting software

	● Employment History ● Disciplinary Records ● DBS		
Volunteers	● Name ● Date of Birth ● Address and Contact Information ● Nationality ● Ethnicity ● Driving Licence ● Car Registration ● Health and Disability Information ● Gender ● Sexual Orientation ● Religious Beliefs ● Marital Status ● Bank Details ● Employment History ● Disciplinary Records ● DBS	● Most of this information is needed to enable us to manage the data subject's volunteering including ensuring we can contact them, meet health and safety requirements, match them to appropriate volunteering opportunities, support them appropriately and pay their expenses. ● We also process some of this data to monitor our volunteer demographics to ensure our volunteer team is reflective of the service users we are supporting.	● Encrypted HR Management Database ● Paper-based volunteer files stored in locked filing cabinets on SAtA premises only ● On "QuickBooks" accounting software
Trustees	● Name ● Date of Birth ● Address and Contact information ● Occupation ● Conflicts of Interest ● Trustee Eligibility Information	● This is data that we need to comply with regulatory and governance requirements set by Companies House and Charity Commission	● Encrypted, password protected drive on SAtA's Server ● Paper-based trustee files stored in locked filing cabinets on SAtA premises only
Job/Volunteer Applicants	● Name ● Age Group ● Address and Contact Information ● Ethnicity ● Health and Disability Information ● Gender ● Sexual Orientation ● Religious Beliefs ● Marital Status ● National Insurance Number ● Employment History ● DBS	● We need this information to make safe and appropriate recruitment decisions for both volunteers and members of staff. ● We use some of the data to monitor the effectiveness of our recruitment advertising and to ensure that we are reaching all those who may wish to work with us.	● Encrypted, password protected drive on SAtA's Server ● Paper-based application paperwork stored in locked filing cabinets on SAtA premises only.
Funders/ Supporters	● Name ● Address and Contact Information	● We use this information to ensure that we can keep our supporters and	● Encrypted, password protected drive on SAtA's Server

		funders informed about our work. ● With their express consent, we may approach previous supporters and funders to request further support.	

Privacy Notices

As part of our commitment to transparency and Data Subjects' "**Right to be Informed**", we publish and provide privacy notices for each of the categories of Data Subject identified above to explain what data we hold, the purpose(s) that we use it for, the lawful basis on which we rely for different processing activities and who we may share the data with among other matters. Privacy notices will also detail the individual rights that Data Subjects have over the data that we hold about them.

Wherever possible and appropriate, privacy notices will be provided prior to the collection or processing of the data to ensure that all Data Subjects are aware of the processing activity and purposes prior to the data being provided.

As far as possible, privacy notices will be written in clear and concise language and will be easy to understand.

Rights of Data Subjects

SAtA recognises and is committed to the rights given to Data Subjects in respect of the Data that we hold about them. Those rights are contained in the GDPR and will be applicable in different circumstances depending on the lawful basis for the processing. The rights available to individuals in respect of different data will be detailed in the relevant privacy notice.

Right of Access

This right entitles individuals to obtain from SAtA a confirmation that we are processing their personal data as well as a copy of all the personal data that we hold along with some additional information.

A request for access to personal data is sometimes known as a "Subject Access Request" (SAR) and such a request can be made either verbally or in writing

(including electronically) and does not have any prescribed format. A SAR can be made to any member of SAtA's staff or to a volunteer and can also be made via our website or social media channels. A request does not have to be labelled as a "Subject Access Request"; it need only be clear that the individual is requesting access to his/her data. Although it is ***not mandatory***, it may help both parties for requests to be made using the Subject Access Request form that is appended to this policy.

When SAtA receives a SAR, the information requested will be provided to the data subject without delay and at the latest within one month of the request having been made. Where request(s) from an individual are complex or numerous, we may extend this timeframe for up to two additional months but we will notify the individual and give them the reason for this within one month.

A SAR may be made by a third party on behalf of the data subject (for example where the data subject lacks capacity) but SAtA will require evidence that the third party has authority to make the request. This may be in the form of a written authorisation or a power of attorney.

Right to Rectification

Whilst SAtA will always make every effort to ensure that data is kept accurate and up-to-date but we also recognise that there may be occasions when individuals identify inaccurate data and in such cases they have a right to request that the information is rectified.

Like a SAR, a request for rectification can be made verbally or in writing (including electronically) and does not have any prescribed format. The request can be made to any member of staff or to a volunteer and can also be made through our website or social media channels.

When a request is received, we will assess the data that we hold to determine if it is in fact inaccurate and we will respond to the Data Subject without delay and at the latest within one month. During that time, SAtA will restrict the processing of that data until it has been determined whether it is accurate or not.

After the assessment, we will either:

a) Amend the data if it is found to be incorrect; or
b) Inform the Data Subject if we consider that the data we hold is correct and that we will not be making any amendments to it.

If we decide not to amend the data, we will:

a) Inform the Data Subject of their right to complain to the Information Commissioner;
b) Inform the Data Subject of their right to enforce their right through judicial remedy;

c) Record a note with the data to indicate that the data subject challenges the accuracy of the data.

Right to Erasure

SAtA will, as a matter of course, erase data in which it no longer has a lawful interest in retaining. This may be because consent has been withdrawn or because the processing is no longer necessary to achieve the purpose among other reasons. This is also related to the data retention table included below under "Disposal of Data".

In addition, Data Subjects may also make a request for data that SAtA holds about them to be erased in certain circumstances, which are:

a) That the personal data is no longer necessary for the purpose for which it was originally collected or processed;
b) Where the lawful basis for processing is consent and that consent is withdrawn;
c) Where the lawful basis for processing is legitimate interest, the Data Subject objects to the processing and there is no overriding legitimate interest to continue the processing;
d) Where SAtA is using the Data for direct marketing and the individual objects to the processing;
e) The Data has been processed unlawfully;
f) The Data has to be erased to comply with a legal obligation.

A request for erasure can be made verbally or in writing (including electronically) and does not have any prescribed format. The request can be made to any member of staff or to a volunteer and can also be made through our website or social media channels.

A request will be responded to within one month of receipt.

Right to Restrict Processing

The purpose of this right is to enable Data Subject to limit how SAtA can process their data in certain circumstances and for certain periods of time as an alternative to permanent erasure.

The right can apply when:

a) There is a question about the accuracy of the data (processing will be restricted until the accuracy of the data has been established);
b) SAtA has processed the data unlawfully but the Data Subject opposes erasure and prefers restriction;
c) SAtA no longer needs to process the information but the Data Subject opposes erasure as they require the data to establish, exercise or defend a legal claim;

d) The Data Subject has objected to the processing and SAtA is considering whether its legitimate interests overrides that objection.

If processing is restricted, SAtA will undertake no processing of the data except to store it.

A request for restriction can be made verbally or in writing (including electronically) and does not have any prescribed format. The request can be made to any member of staff or to a volunteer and can also be made through our website or social media channels.

A request will be responded to within one month of receipt.

Right to Portability

This right enables Data Subject to request that Data held about them be provided with that data in a structured, commonly used, format or for that data to be transmitted to another Data Controller at the request of the Data Subject.

SAtA does not operate automated systems for data processing and as such, this right does not apply to data that we hold. However, we will continue to review the situation and should we commence the use of such an automated system, we will put measures in place to ensure that we comply with these regulations.

Right to Object

Data Subjects can object to data processing depending on the purpose of the processing and the lawful basis. SAtA's privacy notices will detail the rights of various Data Subjects to object to the processing of the data that we hold about them to ensure that all Data Subjects are fully informed.

A request for restriction can be made verbally or in writing (including electronically) and does not have any prescribed format. The request can be made to any member of staff or to a volunteer and can also be made through our website or social media channels.

If an objection is received, we will respond without delay and at the latest within one month.

Rights in relation to automated decisions and profiling

SAtA does not undertake any automated decision making or profiling and as an organisation that is founded on the principle of person-centred practice, we intend never to automate any decision-making processes.

However, we will continue to review this position and if we identify any automated decision-making processes or profiling activities, we will act to ensure that they comply with legal requirements.

Consent

Some (although not all) of the processing that SAtA undertakes requires the consent of the Data Subject. This particularly the case where the processing involves "Special Category Data". Where consent is appropriate, we will ensure that it is:

- **Freely given** (we will make sure that Data Subjects have a genuine choice about if and how their data is used)
- **Explicit** (we will not use "opt-out" consent and)
- **Granular** (we will ask for consent for specific types of processing)
- **Appropriately Reviewed** (we will review consent periodically to ensure it is still valid)
- **Recorded**

As an independent advocacy organisation we are passionate ensuring that consent is genuine and informed and Appendix 1 gives further information on SAtA's view of informed consent.

Storage of Personal Data

Electronic Storage

SAtA uses a cloud-based Case Management Database ("CharityLog") which is a secure system used to record client contact and case information. This system meets the requirements of the GDPR and is encrypted and accessible only by authorised individuals through use of a password. This system is used by all staff and volunteers as the exclusive location of electronic data about clients (including uploaded documents and correspondence). All staff and volunteers receive training on the use of this system and are required to maintain high standards of data recording.

Staff and volunteers should ensure that passwords are kept confidential at all times. In exceptional cases, where it is necessary to divulge a password, immediate steps should be taken to reset the password to ensure the security of the data.

Staff information is stored in our "BreatheHR" system which is encrypted and accessed by password protection. All staff have usernames and passwords for their

own profiles and line managers have access to necessary information about the individuals that report to them. The CEO has access to the records of all staff and may delegate such access to another individual only insofar as that access is required for that individual to carry out his/her role properly.

Personal data should always be stored on the relevant database or exceptionally on SAtA's own secure server. Personal data should not be stored on local computer hard disks or on portable storage drives such as USB sticks.

All individual computers are password-protected.

Documents
Wherever possible, physical documents relating to clients should be scanned and uploaded to Lamplight, (with the originals being provided to the client or destroyed by shredding).

Physical documents that are retained must be kept in lockable filing cabinets. Access to those cabinets will be restricted to those with a need to access them, and they will remain locked at all times.

Staff and volunteers should take particular care to ensure that documents are not left in plain sight and that they are filed as above when not in use.

Staff and volunteers who need to remove documents from SAtA premises (for example to attend a meeting) must ensure that they keep those documents with them at all times. They should not be left unattended (for example by being left in a car) and should not be kept away from SAtA premises overnight.

Any documents relating to staff or volunteers will be stored within the relevant personnel records for that individual. Access to such records will be restricted to the CEO and those with the express permission of the CEO.

Retention of Personal Data

Personal Data will only be retained for as long as it is necessary and SAtA will dispose of data in line with the timeframes detailed in the Retention of Records Table Appended to this policy.

Updating of Personal Data

Any changes to personal information should be updated as soon as is practicable to minimise the risk of using information that is out of date. Staff and volunteers should notify SAtA of changes to their personal data as soon as possible after the change.

Clients' personal data should be checked with them regularly and always prior to the commencement of a new case.

Staff and volunteers' personal data will be checked annually to ensure that it remains accurate and current.

Destruction of Personal Data

When confidential records and data are no longer required they will be destroyed by confidential shredding.

For digital data, destruction means the permanent deletion of the data from SAtA's servers and other systems (such as client database).

When personal data is destroyed, SAtA may retain such parts of it that do not identify the individual concerned but may still have residual uses to the organisation (for example for statistical purposes or to evidence work and outcomes over time). Such data will be pseudonymised to ensure that the individuals are no longer identifiable.

Personal Data Breaches

A personal data breach is a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Staff and volunteers are required to report any actual or suspected breaches to the DPO immediately.

The DPO should investigate the circumstances and decide on any appropriate actions which may include:

- Notifying the Information Commissioner about the breach
- Notifying the data subject(s) affected
- Reviewing security systems and other procedures to ensure further breaches do not happen
- Considering whether the breach requires any further action (for example whether disciplinary action might be necessary)

Training

Confidentiality and Data Protection is a core element of the induction process for staff and volunteers and is included within the Staff and Volunteer Handbooks.

Training will be reviewed every 2 years or earlier if there are significant changes to legislation, case law or to SAtA's own policy and procedures.

Appendix 1 – INFORMED CONSENT

Informed consent is a phrase often used to indicate that the consent a person gives meets certain minimum standards. An informed consent should be based upon a clear appreciation and understanding of the facts, implications, and future consequences of an action.

In order to give informed consent, the individual concerned must have adequate reasoning faculties and be in possession of all relevant facts at the time consent is given. Impairments to reasoning and judgment which may make it impossible for someone to give informed consent include such factors as basic intellectual or emotional immaturity, high levels of stress such as Post Traumatic Stress Disorder; a severe intellectual disability; severe mental illness; intoxication, severe sleep deprivation; Alzheimer's disease or dementia; or being in a coma.

To give informed consent means having all of the following:

- A general understanding of what decision needs to be made and why;
- A general understanding of the likely consequences of making, or not making, this decision;
- The ability to understand, retain, use and weigh up the information relevant to any decision;
- The ability to communicate the decision to others by any means (by talking, using sign language, interpreters, written details or other alternative augmentative communication tools and techniques).

Having mental capacity is the ability to make a decision. This includes the ability to make a decision that affects daily life – such as when to get up, what to wear or whether to go to the doctor when feeling ill – as well as more serious or significant decisions such as where to live, who to marry and what kind of work to do or seek.

It also refers to a person's ability to make a decision that may have legal consequences for them or others. Examples include agreeing to have medical treatment, buying goods or making a will.

A person can give permission, approval or agreement to something without having enough information to understand the process to be used, but he/she does want to know about the risks associated with it.

For example, a person may be happy to take the word of a car mechanic that his/her car needs repairing because he/she does not know enough about cars, or a person may give approval for an operation because he/she trusts the medical professionals to do what is best for him/her because he/she has little medical knowledge.

By the same token if a car mechanic repairs a person's car without telling him/her how much it is likely to cost and just presents him/her with a very large and unexpected invoice, or a person returns from a medical procedure with loss of use of any part of our anatomy and was not warned of the risks or dangers involved in the surgery, that person likely to be very angry indeed because he/she was not a part of the decision-making process.

If the person had known why the vehicle was not working properly, he/she might have asked about the possibility of getting used parts or leaving the repairs to a later date, or if there was alternative medical treatment he/she may have avoided surgery.

When a parent agrees to have his/her child assessed by a psychologist, does he/she know what tests will be used, what they are measuring or how the results may affect the child's placement in the school system? Will there be a report? Who will get copies of it? Will someone explain it?

Assessments for court purposes can be confusing and upsetting if the parties do not have full understanding. Often individuals who are going through child protection procedures or custody battles, for example, think that they can hire a psychologist to state that they would be the best parent for children and therefore should have sole custody. It is easy to assume that paying for a professional will guarantee support for one's case. Psychologists who are involved in custody and access cases focus on the needs of the children and not merely on the parent who has paid for the report.

Informed Consent means knowing in advance what services will be provided and how they will be conducted. Treatment for depression, for example, can consist of Cognitive-Behavioural therapy, hypnotism, medication or a number of other therapies, and a person would need to understand which will be used, how often and in what duration.

The whole area of fees can also be confusing - how much will be charged for services? How will they be calculated? When are is payment expected? Does a person's home have to be sold to pay for residential care fees?

Informed Consent is designed to protect individuals. Being a good advocate means asking questions and ensuring that you, and therefore the person you are advocating for, understand what will happen, how, when, where and the risks that they face. It is important to support service users not to consent to do anything that they do not fully understand. They may end up being horribly disappointed, upset or even changed for life in a way that they would not have chosen.

Solihull Action through Advocacy

Subject Access Request Form

You have the right to request access to any personal data that Solihull Action through Advocacy (SAtA) holds about you. This form is designed to make it easier for you to request access to your data by ensuring that you include all of the information that we need to process your request. You do not have to use this form.

Once completed, this form can be sent either by post to:

The Data Protection Officer
SAtA
11-13 Land Lane
Marston Green
Solihull
B37 7DE

Or by email:

office@solihulladvocacy.org.uk – please use "Subject Access Request" in the subject line

Section 1 – About the Data Subject (the person whose data is being requested)

Full Name:	
Date of Birth:	
Current Address (including postcode)	
Telephone	
Mobile	
Email	

Section 2 – About the person making this request

Are you the Data Subject?	Yes □	No □

If you answered **"Yes"** please go to **section 3.**
If you answered **"No"** please complete the remainder of **section 2**

Full Name:	
Date of Birth:	
Current Address (including postcode)	
Telephone	
Mobile	
Email	

If you are **NOT** the data subject, we will require documentary evidence that you are authorised to make this request on their behalf. This might include a signed authority from the data subject or evidence of a lasting power of attorney.

Please identify below the evidence that you are including:

Section 3 – Evidence of Identity

Please indicate the evidence that you are providing to confirm;

The identity of the Data Subject:	**Your identity (if different)**
□ Copy of Driving Licence	□ Copy of Driving Licence
□ Copy of Passport	□ Copy of Passport
□ Birth Certificate	□ Birth Certificate
□ Council Tax Bill	□ Council Tax Bill
□ Utility Bill (recent)	□ Utility Bill (recent)
□ Other (please specify):	□ Other (please specify):

Section 4 – The Data

Please describe the data that you are requesting access to:

Section 5 – Declaration

I declare that the information given on this form is true and accurate to the best of my knowledge.

I authorise SAtA to provide the details contained in this form as well as its associated attachments and enclosures to such of its staff as may be necessary for the fulfilment of this request.

I understand that if I am not the data subject (or acting on behalf of the data subject with appropriate authority) and attempt to obtain data to which I am not entitled, I may be subject to prosecution under the Data Protection Act 1998 s.55.

Name	
Signature	
Date	

Please return this completed form, making sure to include any documentary evidence that we have requested above, according to the instructions on the front.

Appendix 3

Solihull Action through Advocacy

CONFIDENTIALITY AGREEMENT

Acknowledgement of confidentiality of client & organisational information

I acknowledge that as a Trustee/Staff Member/Volunteer of SAtA I may learn or have access to confidential information about SAtA, its clients, staff and volunteers during the performance of my duties. I have read the *Confidentiality and Data Protection Policy* ("*the Policy"*) and I undertake:

1. To take all necessary steps to preserve the confidentiality and security of such information including all practical and technical measures required by *the Policy*.
2. Only to share confidential information within SAtA on a 'need to know' basis.
3. Never to provide confidential information to any external third party without the express consent of the data subject except insofar as any such breach is sanctioned within *the Policy*.
4. To seek immediate advice from my line manager or from the CEO in the event that I am uncertain about the application of *the Policy* in any given circumstance.
5. To comply with all aspects of *the Policy* and any appendices thereto.

I understand that failure to comply with the requirements of *the Policy* and the terms of this agreement may result in disciplinary action being taken up to and including dismissal in serious circumstances.

Name	
Position Held	
Signature	
Date	

Appendix 4

Retention of Records Table

Who	What	How Long to be Retained	Why
Service Users	Personal and Contact Details Case Files	6 years following the end of a case unless: ●A different period is agreed with the service user during case closure **and/or** ●The service user's file needs to be re-opened during that period **and/or** ●25 years in the case of case-file data relating to safeguarding matters.	It is common for our service users to return for support at a later time, often many months or years after the ending of a previous case. We often need records of our previous involvement in order to inform new cases. We may also need to justify our actions or decisions if we were to be asked to investigate a complaint or a safeguarding matter.
Former Staff	Employee files	6 years from the end of the financial year in which the individual ceased to be an employee. The following will not be retained: ●Emergency contact details ●Bank details	We may require this data to: ●Respond to requests for references ●To comply with audits from HMRC ●To defend legal claims
Former Volunteers	Volunteer files	6 years from the end of the financial year in which the individual ceased to be a volunteer. The following will not be retained: ●Emergency contact details	We may require this data to investigate and respond to complaints or to defend legal claims either from the volunteer or from third parties

		● Bank details	
Trustees	Contact Information Governance Data	Governance Data to be retained permanently (this includes entries in minutes of board meetings as well as information relating to conflicts of interest and eligibility) Contact information to be retained for 6 years following the end of the financial year in which the individual's appointment as a trustee was terminated.	We may need this information to investigate, respond to or comply with regulatory/compliance audits from the Charity Commission, Companies House or HMRC. Some of the information may also be needed to respond to/defend legal claims.
Unsuccessful Job Applicants	● Application forms ● Shortlisting and interview grids ● Correspondence	All to be retained for 6 months.	This is to ensure that we are in a position to defend against legal claims in respect of recruitment activities.
Unsuccessful Volunteer Applications	● Application Forms ● Correspondence	These will not normally be retained	We have no need to retain them and there is no recourse to a volunteer who we decide not to accept.
Funders/ Supporters	● Name ● Address and Contact Information	Until we are notified that the individual no longer wishes for us to hold their details	We hold details of funders/supporters on the basis of consent. We will erase the data if that consent is withdrawn.