Swindon Advocacy Movement

Data Protection Policy

Aim

This policy is to ensure that Swindon Advocacy Movement (SAM) complies with the Data Protection Act 1998 and General Data Protection Regulations (May 2018), including the eight main principles:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

- Ensure the rights of a data subject to access their personal data that the organisation holds while protecting the rights of third parties

Definition of "data" and "data subject"

When this policy refers to "data", this applies to any personal information kept by the organisation for the purposes of processing. This will include written notes and records held in electronic and paper

filing systems.

A “data subject” is a client, worker (employee, volunteer, placement student or agent temp) or other person or organisation that we may hold records on or communicate with.
Personal data is any data relating to a living individual (e.g. name, address, payroll details, etc.). Sensitive data forms personal data and records such things as ethnic origin, religious beliefs, criminal convictions, etc. Data processing occurs whenever data is compiled, stored, or otherwise operated on. Data controller is the person or organisation processing the data.

Where generalised, the policy also includes business sensitive information.

Registration

As a small not for profit organisation, SAM is exempt from registration with ICO. The exemption applies to processing which is only for the purposes of:
- establishing or maintaining membership;
- supporting a not-for-profit body or association; or
- providing or administering activities for either the members or those who have regular contact with it. This includes giving support to individuals.

SAM respects the privacy of data subjects and in connection with the handling of information we will ensure that:

- The CEO is the Data Controller for SAM and as such assumes overall responsibility for data captured and stored
- Everyone managing and handling personal information known as Data Collectors understands the requirements of the Act and their responsibilities under it
- Everyone managing and handling personal information is

appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Queries about handling personal information are promptly and efficiently dealt with
- A regular review and audit is made of the way in which personal information is managed
- Methods of handling personal information are regularly assessed and evaluated.

Responsibilities

This policy applies to all staff, volunteers, trustees or management committees. It aims to set out the broad steps by which personal data is collected, the requirements to ensure records are completed appropriately and the requirements for the handling, storage and destruction of records.

The Trustees have high level responsibility and accountability for compliance with the Regulation, including registration, the reporting of breaches (via the Data Controller) and overseeing broad policy; ensuring it is reviewed regularly. They further review and monitor through the Governance. Day to day operations and procedures are delegated to the Data Controller (CEO) and in turn to senior managers. The Trustees thus delegate compliance on a practical level.

Gaining personal data

Any permission to process client or staff information will be gained at the commencement of any contract, referral or agreement. This includes a completed client consent form with access to SAM Privacy Policy which is published on the SAM website and our Data Protection Policy on request.

Electronic Data

All client data must be recorded on the NAS which includes a case management and reporting tool which stores all client notes and other records including uploading documents and correspondence. This is stored on SAM's central servers via secure network access.

SAM will ensure that all electronic data, including client database entries, emails and letters are accessed and secured by passwords, anti-virus, anti-spyware and firewall software. Personal data should not be stored on a local hard drive or laptop. All emails containing personal data will be deleted on closure of cases.

In line with the SAM procedures, workers are to keep passwords confidential. In extreme cases where it is necessary for the password to be shared, immediate steps should be taken to change the password.

As official documents, emails to any SAM account may be accessed in the absence of the account holder by their manager or as part of a Data Protection Access Request. Subject to an official request, emails may also be monitored for the purposes of quality and monitoring performance or as otherwise specified.

Electronic Communications

We monitor electronic communication by staff, volunteers and clients including to social media and websites, to ensure that these systems are used in accordance with our data protection policies. Staff are required to strictly adhere to the Social Media Policy at SAM.

Files

Filing systems should be kept in a way that respects the information held:

- Hard copies of data must be kept in a lockable filing cabinet or

other secure storage compartment, however wherever possible documents should be uploaded to the Client Database and originals returned to the client or destroyed;

- Workers must ensure that such data is not left in the sight of others and is filed when not in use;

Updating personal data

- Any changes to personal data, such as a new address, should be carried out at the first available opportunity to minimise the risk of using out of date information.

- Checks to ensure correct personal details are current and accurate where a client reopens their case or a worker returns to the organisation after leaving.

Transferring data and use of secure email

Emails are a quick and convenient way of providing or responding to requests for information, although care must be exercised to ensure that confidential or sensitive information is kept secure, therefore it may be appropriate to use encrypted emails depending on the nature and circumstances of the communication.

The email encryption system should be used where there are concerns about sending sensitive or confidential information by email.

We should continue to respond to the needs of individual clients and communicate in the most appropriate way, and this is another device that allows us to respond to concerns about security or privacy.

Private emails for current staff members will not be used.

Sharing data to third parties

All advocacy engagement is subject to our Independent Advocacy Protocol, working with all stakeholders including the voluntary sector "data sharing agreement" within Sanford House.

Data must not be revealed to a third party without the data subject's express consent. However, there may be occasions where data is shared between SAM and selected partners which will be by client consent.

This would only be breached in line with the levels of breach contained in the Confidentiality Policy for example in order to protect the client in the event of a life threatening situation or in issues relating to national security.

Where a subject is not able to give consent to share data advocates must follow MCA and Best Interest checklist to make decision regarding sharing of data. This also must be in line with SAM Non-Instructed Policy and Confidentiality Policy.

Where a third party is in another country, data will only be revealed where equivalent data protection laws exist or where a contracted agreement with the third party is accepted by the client and by SAM.

Staff Records

Staff, volunteers and trustee personal details are restricted and maintained by the CEO and not shared outside the organisation, with the exception of, and for administration purposes, with the Charity's payroll and pension scheme providers, occupational health advisor and bank in respect of payroll and salary information.

Staff and volunteer records are also maintained by the Data Controller in respect of changing health conditions and medicines being taken purely to ensure we deal appropriately with any incident or accident at work. This will be with the data subject's consent.

References

It is SAM's policy to provide references regarding the employment of current or past employees and volunteers when requested by another employer or potential lender. All references should remain factual and resist giving opinions of the referee or other staff members which cannot be backed up by evidence.

Former or existing staff can request to see these references under the Data Protection Act. All reference requests should be directed to the CEO for a response.

Data Protection Requests

Data subjects have the right to access personal data which is held by the organisation, both files and electronic data.

Where clients have an open file with SAM a copy of any relevant documents or of the complete file can be provided on request.

If the data subject believes that the information we hold on them is inaccurate then they are entitled to ask for it to be amended.

All data subjects under Article 17 have the right to be forgotten. If the subject is no longer working with a client of the charity, SAM will delete all identifiable data being held immediately upon request.

If the requests concern a closed case then an official request is needed, describing the exact request and providing proof of ID, SAM has one month to reply to such requests. No fee is charged for a request, although we reserve the right to make a charge where there have been multiple requests.

When fulfilling the request, SAM must take into consideration any data that has third party involvement. Data can be withdrawn if:

- the third party has not given consent for the data subject to see the data;
- the data would lead to the harm of the data subject or third party

Please refer to the Data Protection Subject Access Request Procedures, and in particular the:-

Subject Access Request Form
Subject Access Request Procedure and Guidelines
On the occasion that a relative, solicitor or other third party makes a subject access request on a subject's behalf, either because the subject lacks capacity or is deceased, SAM will require evidence that such a person is formally acting on their behalf.

Such requests will be reviewed on a case by case basis to determine whether such data can be released to the third party but will require proof of identity and a copy of power of attorney.

Where the data subject is deceased there is no automatic right to supply information, however where the individual can provide a copy of their own proof of identity and the grant of probate or certificated copy of the last will and testament, their request will be considered.

Protecting third parties

In meeting a data subject access request it is important that personal data relating to other identifiable individuals mentioned in the documents should not be revealed unless permission for disclosure is given by the individuals concerned. The data subject enquirer has a right to see comments made about them but the identity of the individual who made those comments should not be revealed without their express permission.

Secure file transfer

Transfers of sensitive information outside the organisation should normally be sent via encrypted email, Egress or Adobe Acrobat, after first confirming the email address is the correct address of the intended recipient.

End of a contract

When a contract for services ends, there be a legal obligation on SAM to work with any new provider of the service, and SAM will work with them to ensure any open cases are transferred to the new provider providing the client or, for clients that lack capacity, the initial referrer, consents. Clients will receive written notice that a change is taking place and their consent to their data being transferred will be sought.

In the event of a loss of an existing contract or a new contract bid is successful, the terms of the contract may stipulate that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (commonly known as TUPE) apply. In this situation, SAM is obliged to share/receive specific data about workers under these terms.

Data retention, archiving and destruction

Data is retained only for as long as the needs of the original consent for which it was collected and in line with any retention periods required in case of query, or to satisfy regulatory or contractual requirements.
By client information we mean any information that could identify the client as an individual or could be used to inform any decision about them.

When we no longer need to keep a client file we will delete the client's contact details, any associated documents, and any other information that could identify the client personally. We may keep other information about the case where this cannot identify the client personally but is required for contractual or operational reasons.

By deletion for electronic records we mean put “beyond use” as defined by the Data Protection Information Commissioner’s Office guidelines, and paper records are archived in secure storage and destroyed by shredding according to the time periods given in Appendix 1 – Data Retention Periods.

Security Breaches

SAM must report security breaches to the Information Commissioner (ICO) and the Charity Commission, if it is believed that data is at risk of being misused as a result of loss of data. All possible breaches will be recorded by SAM. It is the employees’ responsibility to inform the loss or possible loss of data to:

- CEO
- Line manager or another senior manager within SAM

Copyright Information

Copyright is a legal right to control the use and exploitation of original creative material. Copyright in a work is usually owned by its creator. We need be aware of this when using non-original material such as photo and permission sought for its use. Copyright material such as photos, newspaper articles or other documents should not be reproduced.

Photographs and Video

All staff, volunteers, trustees and clients will be asked to confirm if they agree to their image being used for marketing and fundraising purposes. We will request consent before taking any photographs or videos of individuals and will let them know how any photographs or videos of individuals will be used i.e. Website and social media.

Data Protection Audit

An audit of current data, both manual and electronic must take place

quarterly and recorded on the SAM Asset Register.

This will involve checking whether the data should still be kept under the retention periods stated on the next page. When data is due to be destroyed after it has reached the end of its retention period, this should be done so that the document cannot be used again (i.e. files are shredded, computer files and database entries are deleted).

Managers must then report back to the CEO to confirm this has been done for their office/project.

Marketing

SAM maintains a members and supporters database which is regularly updated to ensure that data subjects are still agreeable to receiving information about our services, charity events and fundraising activities. This is a mix of clients, volunteers, trustees, supporters, donors and carers.

All contacts have the opportunity to “opt in” and specify what information they would like to receive from us and how we communicate this to them i.e., email, telephone, letter. Information may include for example, newsletters fundraising and event calendars, information packs, service updates, etc.

We will inform individuals how and by whom their information will be used when they give consent to us holding their data.

SAM will not make unsolicited email or phone calls to any organisation or individual who has told us they do not want our communication, or to any number on the Telephone Preference Service list. We will not send unsolicited fax marketing to anyone who has a number on the Fax Preference Service, or who has hold us they object.

In all our marketing we will identify who we are and provide contact

details, postal address, email address, charity number and phone number so that the recipient can contact us.

If an individual decides they no longer want to receive marketing, we will deal with their request promptly and inform the relevant personnel.

Retention Periods

SAM adheres to the statutory retention periods for worker, financial and health and safety data. Examples are outlined below:

Record	Retention period
accident books, accident records/reports	12 years
accounting records	7 years
Client files	6 years
Payroll records	4 years from tax year relate to
Worker records including supervision notes.	6 years after the worker has left
Volunteer files	4 years after finishing volunteering
Grievance/disciplinary records	5 years from end of employment

Application forms and interview notes	Duration of employment for successful application as per worker records and 6 months for unsuccessful applicants
Electronic timesheets/leave	3 years
Meeting minutes (Board and Team)	Indefinitely
Supervision notes	6 years after the worker has left
Emails (SAM Core Depts)	1 year
Exceptional files*	Indefinitely

Exceptional files include, but are not limited to criminal, investigational or national security data that are specifically excluded from this policy.