SYSVP GDPR & Data Protection Policy

South Yorkshire
Sexual Violence Partnership

Introduction 2
Data Protection and the GDPR Principles 3
Security of Information 4
Individual's Rights in Relation to their Personal Information 5
The right to be informed 5
The right of access (subject access request) 6
Subject Access Requests from Police 7
The right to erasure 7
Contact details 8
Appendix A – Processing Documentation 9
Provision of client data 9
Information categories, storage and use 10
Information 10
Storage 10
Purpose 10
Sharing information 10
Retention of information 11
Appendix B - Staff information 12

Introduction

South Yorkshire Sexual Violence Partnership (SYSVP) is a registered charity, commissioned by the South Yorkshire Mayoral Combined Authority (SYMCA) to deliver the South Yorkshire Independent Sexual Violence Advocacy (ISVA) Service.

SYSVP is registered with the Information Commissioners Office (ICO ref. ZB556546) and each SYSVP partner has individual registration:

- Barnsley Sexual Abuse & Rape Crisis Services (BSARCS) – ICO ref. Z344654X
- Doncaster Rape & Sexual Abuse Counselling Service (DRASACS) – ICO ref. Z1632661
- Rotherham Abuse Advocacy & Counselling Service (ROTHACS) – ICO ref. ZA107702

This document details the partnership's fulfilment of its obligations, in relation to the delivery of the South Yorkshire ISVA service, as set out in the Data Protection Act 2018 which sits alongside the General Data Protection Regulations (GDPR), both of which came into effect in the UK on 25 May 2018.

The policy details the obligations of partners when dealing with the personal data of clients accessing the South Yorkshire ISVA service, demonstrating our compliance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) (our '**accountability**').

Each provider will comply with their own individual GDPR policy and procedures in relation to the personal information and/or data held in the delivery of any other (non-ISVA) service provision.

This policy and SYSVP's methods were last reviewed in July 2026 and will be reviewed annually and in response to any change in legislation, regulation and good practice at which time SYSVP will review its methods of collecting, storing and processing of personal data.

Data Protection and the GDPR Principles

Data protection principles apply to the processing (collection, recording, storage, use, analysis, combining, disclosure or deletion) of personal information or data of any identifiable living person.

In GDPR, a 'data controller' is a body which determines the purposes and means of processing personal data and is ultimately responsible for compliance with the UK GDPR. A 'data processor' is responsible for the processing of data, on behalf of the data controller. In relation to the commissioned ISVA service, SYMCA is the 'data controller' and SYSVP the 'data processor'.

The partnership has a named individual who is responsible for dealing with data queries and for ensuring compliance with data protection regulations.

SYSVP will routinely provide specific, anonymised client data and service delivery information to SYMCA on a quarterly basis as part of the agreed performance management and monitoring framework; SYSVP will also comply with any additional requests for ISVA data from its commissioner.

SYSVP must seek permission from SYMCA to report (anonymised) ISVA client data externally, for example information relating to demographics, categorisation of sexual offences and client outcomes, when approaching external funders/partner agencies and when communicating with the wider public in an effort to increase awareness of the impact, nature and incidence of sexual harm.

SYSVP will also report any specific GDPR activities relating to ISVA clients, such as actioned 'subject access requests' and record deletion, as agreed with the SYMCA commissioning manager.

The GDPR sets out seven key principles which are central to the protection of personal information. These principles and how we will comply with them is set out below:

- The principle of ***'lawfulness, fairness and transparency'*** – there must be valid grounds for collecting and using personal data and it must only be used in a way which is fair to the individual. Additionally, an organisation must be clear, open and honest with people from the outset about how their personal data will be used in order that they can make a decision about whether they wish to enter into a relationship with the organisation. *Consent is explicitly sought before a client's personal information is processed by SYSVP, whether this is from the individual directly or confirmed to have been sought from the client by a referring agency.*
  Where a referral is received by automatic data transfer (ADT) from South Yorkshire police (SYP), on the lawful basis of 'public task', we will confirm with the client whether they consent to SYSVP processing their personal information and, where this consent is not provided, their details will be deleted from SYSVP's records and SYP notified.
- The principle of **'purpose limitation'** - the organisation must be clear from the outset on what data it intends to collect and for what purpose. It must also clearly *state* its purpose in order to be accountable and to ensure that individuals are able to

understand how their data is to be used, are able to make decisions about what data they wish to share and assert their rights relating to their data. *The processes and purposes of data collection are set out in the appendices to this policy.*

- The principle of **'data minimisation' -** the data collected by the organisation must be sufficient for it to carry out its intended purpose but must be limited to that which is necessary and should not include irrelevant details. Any individual has the right to request that the organisation rectify inaccurate data or delete any data which is not necessary for the purpose of the organisation. *SYSVP will only record information which is relevant to the service being delivered, the quality and appropriateness of case records is closely monitored by our service leads. The process by which a client is able to exercise their right to erasure is detailed further in this documentation*.
- The principle of '**accuracy**' – an organisation must take all reasonable steps to ensure that any personal data held is accurate and an individual has the right to request that information be rectified where it is not. *SYSVP will respond to any request by an individual for us to rectify information held about them which is incorrect and, where appropriate, make the necessary changes.*
- The principle of **'storage limitation'** – an organisation must not hold data for longer than is necessary for its intended purpose. *Having regard to the relevant statute, regulations and good practice guidance SYSVP will retain client's personal information for 75 years from the date of their last contact unless a client exercises their 'right to be forgotten' (see below).*
- The principle of **'integrity and confidentiality' (security)** - an organisation must process data in a manner which ensures appropriate security of the personal data, using technical and organisational measures to prevent unauthorised access, accidental loss, destruction or damage. *These measures are set out below (Security of Client Information).*

Security of Information

SYSVP partners use servers which are data secure, maintained by a specialist provider and backed up regularly.

All employees, volunteers, trustees, consultants, partners or other parties working on behalf of SYSVP will be made fully aware of both their individual responsibilities and SYSVP's organisational responsibilities in regard to the protection of personal data.

Any data breached must be addressed locally and reported immediately to the contract management team in order that, where appropriate, the breach is reported to the Information Commissioners Office (ICO).

Identifiable and personal client data is held by SYSVP in a secure client record management system (CRMS). Only authorised users are given access to client data and each individual's CRMS user account is secured by a unique password. Accounts are disabled promptly when an individual's employment ends.

SYSVP employees must comply with the following measures for protecting client's personal data:

- Personal data must only be transmitted over secure networks
- All passwords used to protect personal data should not be shared, should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.
- Passwords should not be saved in the browser if others have access to a shared computer, nor should they be written down where they may be easily accessed by others.
- SYSVP recommends the use of 'three random words' passwords and that multi-factor authentication (MFA) is in place wherever possible.
- Personal information contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely in the client's case management record. The emails should be deleted at the first opportunity
- All hardcopies of personal information should be stored securely in a locked drawer or cabinet.
- Employees must ensure that information which may identify a client is not left on their desk, on the photocopier or elsewhere at the end of their working day.
- Where possible, employees should refrain from taking a client's personal information away from their place of work. However, where this is unavoidable or impractical, the information taken should be the minimum required to undertake the necessary work and should not include identifying information. Furthermore, this information must be kept securely and must not be left unattended (i.e. in a vehicle).

Each partner will hold the personal and identifiable information of their staff team in secure HR management systems and, where paper records are held, these will also be stored securely; some information will be routinely shared with the SYSVP contract lead/ commissioner in order for the performance of the partnership's obligations (see Appendix 2).

The partnership has a shared drive, held on a secure SharePoint platform; this has been created as a central point for documents relating to the governance, management and delivery of the South Yorkshire ISVA service. Access to the shared drive is by invite only and is administered by SYSVP's lead partner as part of their contract management responsibilities.

Individual's Rights in Relation to their Personal Information

The GDPR provides, amongst other rights, the following rights to an individual:

- The right to be informed
- The right of access
- The right to erasure

The right to be informed

A key requirement of GDPR is that individuals have the right to be informed about the collection and use of their personal data.

An organisation must provide individuals with information, including, the purposes for processing their personal data, retention periods for their personal data, and who it will be shared with ('privacy information').

An organisation must provide privacy information to individuals at the time their information is collected; if information is provided by other sources (such as in a referral made by a third party), the organisation must provide individuals with this privacy information within a reasonable period and no later than a month.

SYSVP will ensure that our privacy information is clear on our public-facing website and referral portal and, in all cases, will issue privacy information (in a privacy statement) to all new clients which confirms how we will use their data and details their rights relating to their data.

The right of access (subject access request)

Individuals have the right to access their personal data. This is commonly referred to as 'subject access'.

Our clients may make a subject access request (SAR) for their ISVA records verbally or in writing to any individual within the partnership; upon receipt this request should be passed to the SYSVP Data Protection Officer, who will log and acknowledge the request in writing.

The rights of access apply equally to adults and children; a child may request access to their records where they are competent to do so. A parent or guardian may only exercise the right to access on behalf of a child, in considering such requests, SYVP will have regard to:

- whether the child authorises them to do so
- whether the child has sufficient understanding to exercise the right him or herself, or
- whether it is evident that this is in the best interest of the child

Records will only be released to a parent/guardian where we are confident that this does not put the child at risk. Due to the complexity of subject access requests made by a parent or guardian, any such requests will be given careful consideration by SYSVP.

It is also possible for a third party to make a subject access request on behalf of, or in relation to, an individual but, in order for us to consider this, they must provide written evidence of our client having given consent to the request being made.

In all cases, SYSVP will liaise directly with our client to confirm their consent to their personal information being released, ensuring that they are able to make an informed decision about the provision of their records.

The only exception to this is in relation to requests made by a Judge overseeing Court proceedings (in which case a client will be informed of our responsibility to comply).

Prior to any records being released an appropriate manager will confirm that the content is appropriate for sharing in its entirety, redacting third party information.

For the purpose of transparency, SYSVP will allow the client to view the record prior to release to a third party, though careful consideration will be given where a client has made

early disclosures to SYSVP and is considering reporting to the police and/ or providing an ABE or written statement.
Where the content is particularly sensitive it may be appropriate for us to meet with the client to go through the records prior to release.

The SYSVP Data Protection Officer, as part of the contract management team, will ensure that the SYMCA commissioning manager is informed of any subject access requests and subsequent action taken.

SYSVP must respond in full to a SAR within 30 days of the request having been made and, where information is provided, will not charge a fee unless it is deemed 'manifestly unfounded or excessive', where we may charge a reasonable fee for the administrative costs of complying with the request (this fee will be dependent on how much work is involved and how many copies are requested, but will not normally exceed £25).

Subject Access Requests from Police

Requests for records from the police must be submitted on the Third Party Material (TPM) request form, mandated by the National Police Chiefs Council. Where a request is made in any other manner, we will advise that the request has been rejected, outlining the requirement to submit a request on the mandatory TPM request form.

The TPM request form will confirm that the client has consented to their records being provided to the Police but, in all cases SYSVP will contact the client to confirm they still consent to the records being provided and, if consent is withdrawn, contact the OIC detailed on the form to advise of this.

The TPM request form requires full reasoning for the request having been made (specifically why there is a belief that the records contain material which is relevant to an investigation and that the request is necessary and proportionate) and will be signed by an Inspector (or equivalent) confirming that the completed request meets the required thresholds.

Generally, where a client has consented to the provision of their records to the police, it is not appropriate to restrict/choose the information made available to the police (although it may be appropriate to redact third party information). This is because the provision of partial records may prevent the police from discharging their disclosure obligations; may be detrimental to the prosecution case; and may aid the defence case (i.e. leaving potential for the defence to argue that the defendant is not given a fair trial); this highlights the absolute need for case records to contain only information which is relevant to the provision of support.

The right to erasure

GDPR introduces the right for an individual to have their personal data removed. This is often called the 'right to be forgotten' and is essentially an individual's withdrawal of consent for an organisation to process their data.

Our clients are able to make a request for their personal data to be deleted verbally or in writing to any employee within the partnership. Upon receipt this request should be passed to the Data Protection Officer who will log and acknowledge the request in writing.

In considering a client's request for erasure, we will consider whether the interests of SYSVP exceed that of the client and may decide to refuse the request, either fully or in part (i.e. it may be appropriate just to retain information pertinent to the delivery of any future services for example where a client has created a risk for staff or the organisation).

The final decision and action taken must be notified to the individual making the request within 30 days of the request having been made.

The SYSVP Data Protection Officer, as part of the contract management team, will ensure that the SYMCA commissioning manager is informed of any subject access requests and subsequent action taken.

Contact details

SYSVP Data Protection Officer: Rebecca Richardson

Correspondence address: SYSVP, P.O. Box 775, Barnsley, S70 9PL

Email: SYSVP@bsarcs.org

Appendix A – Processing Documentation

All client information is recorded, processed and retained on the basis of consent. However, there may also be a legitimate business interest in retaining certain identifying data and this will be considered in the case of any request for access and erasure (for example what is pertinent to risk and appropriate service delivery).

Provision of client data

Referrals into the SYSVP ISVA service are managed through an on-line, secure referral portal which is monitored and managed by the SYSVP contract lead.

Clients are able to self-refer to the ISVA service by completing the on-line referral form. Where a client wishing to access ISVA support contacts their local service by telephone, the individual taking the call should complete the referral form on behalf of the client.

A third party may also refer through the on-line referral form (any third party professional wishing to make a referral should be directed to this referral portal). Where referral is made by a third party, they must confirm that they have sought explicit consent.

Where a victim is referred to SYSVP by South Yorkshire Police through automatic data transfer (ADT) we will contact the client to confirm that they consent to us processing their data, deleting all of their personal information where this consent is not obtained.

Where a client referred to the ISVA service is a child or young person, we will generally require the consent of their parent or guardian and also require their contact details in order to accept and process a referral.

We will accept a referral for an individual aged under 18 years without the consent of their parent/guardian ONLY where:

- they seek support independently, and
- they are mature enough to be able to make their own decisions (for further information, follow this link)
- acceptance of the referral does not breach our safeguarding protocols and policies

Where a referral is received into the SYSVP referral hub, the contract lead, who holds responsibility for managing referrals will confirm that the information provided is complete, appropriate and that, where necessary, explicit consent has been provided by the client before any client data is processed.

Information categories, storage and use

Where a referral is accepted, the client and referrer information will be added to the South Yorkshire ISVA Service client record management system (CRMS)

Information	Storage	Purpose
Personal information: name, address, date of birth etc. Emergency Contact information.	Secure referral portal. SY ISVA CRMS	Referral management. Communication. Identification. Safeguarding Reporting.
Demographics (gender, ethnicity and vulnerability data	Secure referral portal. SY ISVA CRMS	Monitoring for reporting (anonymously as qualitative data)
Specific categorisation of incidents under Sexual Offences Act 2003	Secure referral portal. SY ISVA CRMS	Monitoring for reporting (anonymously as qualitative data)
Information provided by criminal justice agencies	CJSM secure email system SY ISVA CRMS	Case management Risk management
Interactions with client and partner organisations	Recorded and stored on SY ISVA CRMS	Case management Risk management
Outcomes of involvement (impact reporting)	SY ISVA CRMS	Monitoring for reporting (anonymously as qualitative data).
Service user feedback	Captured using online platforms (i.e. Microsoft forms) – no identifiable data	For reporting purposes

Sharing information

We will not, without consent, share any information about a client unless we are compelled to do so by legal process (summons), there is an overriding safeguarding issue, or it is deemed to be in the best interests of the client (as detailed in our Safeguarding & Confidentiality policies). In these circumstances, we will take all reasonable steps to inform the client of the request made and the information to be shared.

As our ISVA service works with children and vulnerable adults, it is important to acknowledge that we will work closely with parents, caregivers and other agencies involved in supporting our clients. We will be clear with individual clients (and any involved third parties) from the outset as to which agencies we will be involving in our support and all information sharing will be proportionate and only shared where it is appropriate, agreed and deemed to be in the best interest of the client.

Retention of information

All ISVA client data will be stored for 75 years after the last interaction with our service.

However, any client is able to make a request for their personal information to be removed and we will follow the procedures set out in the GDPR & Data Protection Policy to respond to that request.

Appendix B - Staff information

The South Yorkshire Sexual Violence Partnership (SYSVP) is a regional partnership, comprising partner organisations based in Barnsley (BSARCS), Doncaster (DRASACS) and Rotherham (ROTHACS).

SYSVP does not employ staff but does require that the partner organisations share employee information in order for the partnership to meet its obligations and to comply with staff vetting requirements.

In addition to Disclosure and Barring Service (DBS) checks, all individuals involved in the delivery of the South Yorkshire ISVA contract are subject to security vetting.

Partners agree to provide SYSVP (and its commissioners) with the following personal employee information:

- Full name
- Home address
- National Insurance Number (NINO)

This information is required for the purpose of submitting a vetting clearance certificate and should be deleted once vetting is approved.

SYSVP will retain copies of employee vetting and training certificates on the shared drive whilst ever that individual is employed to deliver ISVA services (whether directly or indirectly) but will be deleted when this role ends.

SYSVP may provide the commissioner of the ISVA service with staff information as is necessary for the performance of its obligations (i.e. name, role and evidence of qualifications) and in the event of TUPE arrangements.

We will notify the commissioner when an employee leaves their role in order that their records are updated and vetting clearance can be revoked.

This information is held on a secure SharePoint site; access to this information is limited to the leadership and contract management team.