Data Protection and Privacy Policy and Procedures

Written By: Sarah Lungley	Date: 6 July 2022
Signed and agreed by the trustees:	Date: 21 May 2018
Review Due: July 2025	

A. Data Protection & Privacy Policy

1. Introduction

i. Suffolk Rape Crisis's (SRC's) Data Privacy and Protection Policy and Procedures comply with the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA 2018). For the purposes of data privacy and protection, the people about which SRC holds information are referred to as **data subjects.**

ii. Data privacy and protection applies to **personal data** - any information about an individual from which that person can be identified. It does not include data where the individual's identity has been removed (anonymised data).

iii. SRC's Board of Trustees and Senior Management team are committed to ensuring that SRC complies with all relevant UK GDPR laws around personal data, and to protecting the rights and freedoms of individuals whose information SRC collects in accordance with the General Data Protection Regulation (GDPR).

iv. To ensure this, SRC has developed and implemented documented Data Privacy and Protection procedures. These procedures will be reviewed regularly.

v. According to the UK GDPR, SRC is considered both a **data controller** and a **data processor.** As a **data controller,** SRC determines the purposes and means of processing personal data. As a **data processor,** SRC is responsible for processing personal data on behalf of a controller – which on occasion, SRC may do for partners, commissioners and other agencies. SRC has specific legal obligations to maintain records of personal data and our processing activities. SRC have legal liability if we are responsible for a data breach.

2. SRC collects and uses personal information about our clients for the following purposes:

i. To deliver our services and ensure that the service we deliver is appropriate to the client's needs.

ii. To communicate with other professionals and third parties (e.g., police, social workers, health professionals) to ensure our clients receive the support they need. SRC will only do this with the **specific written consent** of the client, unless there is a legal requirement to share information, or are concerned about the safety of a client or the safety of others.

iii. To report back to SRC commissioners, funders and others about the services SRC offer and the need for services. For this purpose, client data will always be anonymised and is therefore not classed as personal data.

3. SRC collects and uses personal information about our workers for the following purposes:

i. To perform the contract we have entered into with our workers.

ii. To comply with legal or regulatory obligations.

iii. Where it is necessary for SRC's legitimate interests (or those of third party) and the workers' rights do not override those interests.

SRC will:

i. Only hold information about clients and workers for specific purposes.
ii. Inform clients and workers what those purposes are and if those purposes change.
iii. Not hold or process information about individuals without their knowledge.
iv. Only share information about individuals with their consent, unless there is a legal or regulatory obligation to do so, or we are concerned about their safety or the safety of others.
v. Respect the rights of individuals, specifically:
    - The right to be informed.
    - The right of access.
    - The right to rectification.
    - The right to erasure.
    - The right to restrict processing.
    - The right to data portability.
    - The right to object.
    - The right not to be subject to automated decision-making including profiling (this does not apply at SRC).
vi. Ensure that personal data is:
    - Kept safely.
    - Accurate and up-to-date.
    - Not retained once it is no longer required for its stated purposes.
    - Not disclosed to other organisations or to individuals *except* where this is a legal requirement, where consent to share information has been given, or where the information is publicly available elsewhere.
vii. Ensure that breaches of data likely to result in a high risk to the rights and freedoms of individuals are reported to the Information Commissioner's Office (ICO).
viii. Consider the need to protect young women aged 14 – 17 from the outset in all data processing.

4. Data protection responsibilities

i. SRC's CEO has overall responsibility for data protection compliance and is the **Data Protection Officer.** SRC's Office Manager is the **Deputy Data Protection Officer** and will take responsibility for data protection in the Data Protection Officer's absence.
ii. All data privacy and protection queries should be directed to the Data Protection Officer, or in her absence the Deputy Data Protection Officer.
iii. The Data Protection Officer is accountable to SRC's Board of Trustees for the management of personal information within SRC and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

B. Data Privacy and Protection Procedures

1. Communicating Privacy Information

Clients

i. All SRC clients will be provided with privacy information, telling them about the way in which SRC uses, discloses and manages their data at the earliest possible opportunity.

ii. Privacy information will be communicated at all points when data is gathered and on request. Privacy information is also available on SRC's website.

iii. Privacy information will be conveyed using concise, easy to understand and clear language.

iv. Privacy information will be conveyed verbally, and in writing through the ***Confidentiality Agreement, the Outreach@SRC Working Together Agreement, and the Terms & Conditions for Counselling***. The information to be conveyed will include:

- Our purpose and lawful basis for processing data.
- Our data retention periods.
- The rights of data subjects.
- That individuals have a right to complain to the ICO if they think there is a problem with the way SRC are handling their data.

v. All staff will be trained in understanding the necessity of communicating privacy information to our clients, and the keys points to be communicated.

Workers

i. Privacy information will be communicated to all SRC workers, including paid staff, sessional workers and volunteers, at all points when data is gathered.

ii. Privacy information will be conveyed using concise, easy to understand and clear language.

Iii. Privacy information will be conveyed verbally and in writing through *Confidentiality Agreement, the Outreach@SRC Working Together Agreement, and the Terms & Conditions for Counselling.*

2. Consent

Clients

i. We will only share information about individuals with their consent, **unless there is a legal or regulatory obligation to do so, or we are concerned about their safety or the safety of others.**

ii. Consent will be given through signing ***Confidentiality Agreement, the Outreach@SRC Working Together Agreement, and the Terms & Conditions for Counselling****.*

iii. Clients may select which agencies and individuals they consent for us to share information with.

iv. Young women aged 14 or over will be asked to consent to SRC sharing information about them.

v. Signed consent forms will be kept electronically in SRC's secure database.

vi. Consent to share information may be withdrawn at any time.

3. Data Storage and retention

i. Personal client data in a form which permits identification of clients will be retained for 5 years, after which it will be pseudonymised. The data will then be anonymised after a further 2 years.
ii. If the data subject is a child the file will be kept until the child is 25 (this is seven years after they reach the school leaving age) (Information and Records Management Society (IRMS), 2016).
iii. Anonymised client data, for statistical purposes will be kept indefinitely.
iv. Personal workers data will be retained for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements.
v. SRC will, as far as possible, ensure that data is accurate and up to date. If data subjects request that personal data is updated, rectified, or erased this will be done within 1 month of the request.
vi. SRC will ensure the security of all personal data. Data is stored in a purpose-designed database, locked filing cabinets and secure online files which are only accessible to specified staff and volunteers.
vii. Once data is no longer required for its stated purposes and in line with specified retention periods, database records will be archived, and paper records will be shredded in-house.

4. Processing personal data

i. Information about data subjects will not be disclosed to other organisations or to individuals except where this is a legal requirement, where consent to share information has been given, or where the information is publicly available elsewhere.
ii. Data subjects are entitled to see information held about them by SRC, upon written request. The exception to this is where disclosure of information might result in 'serious harm' to the data subject, or a third party. There will be **no charge for requests** and SRC will comply with requests **within one month from the date the written request is received.**
iii. Under certain circumstances, data subjects have the right to object to, block or suppress data processing. This right applies where an individual contest the accuracy of the personal data, where an individual has objected to the processing or when processing is unlawful, and the individual opposes erasure and requests restriction instead.
iv. Data subjects have the right of erasure/'the right to be forgotten'. The right to erasure applies 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 to the processing and there is no overriding legitimate interest for continuing the processing, when personal data was unlawfully processed (i.e., otherwise in breach of the GDPR).
v. SRC will consider requests to suppress processing or for erasure on a case-by-case basis.
vi. In the case of young women, SRC will pay special attention to situations where a young woman has given consent to processing and they later request erasure of the data

(regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a young woman may not have been fully aware of the risks involved in the processing at the time of consent.

vii. In cases of suppressed processing or erasure, when SRC has disclosed the personal data in question to others, SRC will contact each recipient and inform them of the erasure/suppressed processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, SRC will also inform the individuals about these recipients.

viii. Data subjects have the right to have their personal data moved, copied, or transferred to another service. The information will be provided free of charge. A log will be kept as evidence of requests and actions. Explicit consent must be provided before data is moved, copied, or transferred. Data will be securely transferred, using secure e-mail, password protected documents or by being collected in person by a named official.

ix. Records of all subject access, suppressed processing or erasure requests with be kept in a data subjects request log, including evidence of request and action taken.

5. Data Breaches

i. Breaches of data likely to result in a high risk to the rights and freedoms of individuals (for example if they could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage**)** will be reported to the Information Commissioner's Office (ICO).

ii. All workers will be made aware of what constitutes a data breach and must report incidents to the Data Protection Officer. Decisions as to whether a breach is likely to result in a risk to rights and freedoms will be made by the Data Protection Officer, in consultation with the data controller, if this is not SRC.

iii. Records of data breaches will be kept in a data breach log, only accessible to Data Protection Officer and Deputy Data Protection Officer.

6. Young women (aged 14 and over)

The need to protect young people will be considered from the outset in all data processing. All the procedures above apply to processing young women's data, as well as a sense of fairness.

i. Young women aged 14 or over will be asked to consent to SRC processing their data. Using clear, age-appropriate explanations, we will ensure that subjects understand who we are and how we intend to use this data.

ii. Young people have same rights as adults: These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

iii. An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a young person.

7. Data Protection Impact Assessments (DPIAs)

A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. SRC will undertake a DPIA for any major new project which requires the processing of personal data. The DPIA will:

- describe the nature, scope, context, and purposes of the processing.
- assess necessity, proportionality, and compliance measures.
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

If SRC identifies a high risk that cannot be mitigated, the Data Protection Officer will consult the ICO before starting the processing.

8. General

i. In situations where SRC works in partnership with other organisations, including funders, commissioners, and project partners, SRC will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data which SRC has collected. If SRC is acting as the Data Controller we will ensure contracts with data processors comply with GDPR.

ii. All staff and volunteers will be given training on SRC's Data Privacy and Protection Policy and Procedures, including communicating privacy information, safe storage and management and process for data breaches.

iii. SRC's Data Privacy and Protection Policy and Procedures will be reviewed every three years, and/or in response to changes in data processing or legislation.

iv. SRC is registered with the Information Commissioner's Office as **Suffolk Rape Crisis**.

Please refer also to the following SRC documents:

Data privacy and protection for SRC workers (contracts, confidentiality agreement, handbook)
Terms & Conditions for counselling
SRC Referral Form

- End -