Devon Rape Crisis & Sexual Abuse Services

Data Protection Policy

1. Policy

1.1. DRCSAS is committed to applying the highest level of security and protection to the data we hold. This includes all paper records as well as electronic data storage. Data is to be protected in accordance with the procedures below and shared only where necessary, on a need to know basis, and only after we have verified the identity of the individual seeking access to the data.

1.2. The Data Protection Act 1998 and the General Data Protection Regulations (GDPR) require that personal data is protected by appropriate security measures to guard against:

- Unauthorised access, disclosure, alteration or destruction of personal data
- The accidental loss or destruction of personal data ('personal data' being data relating to an identifiable living person)

1.3. In the event that civil proceedings are brought against a data user, it will be a defence to prove that 'reasonable care' was taken to prevent the loss, unauthorised access, alteration, disclosure or destruction of that personal data. The purpose of this policy is to ensure staff protect and secure personal data on systems for which they are responsible.

2. Policy Family

2.1 This Policy should be read in conjunction with the following policies and procedures;

- Data Security and Information Technology Policy
- Document Control and Data Retention Procedure
- Third Party Request Procedure
- Procedure for Processing Subject Access Data Requests
- Breath HR policy
- Business Continuity Plan
- Environment and Sustainability Policy
- Financial Regulations
- Disciplinary and Dismissal Policy and Procedure

3. Security Principles

3.1. Registration. DRCSAS is registered as a Data Controller with the Information Commissioner.

3.2. The Data Protection Officer is the Chief Executive Officer.

3.3. Designated individuals. The following individuals are responsible for owning data and ensuring business is transacted within an acceptable level of risk for the areas identified: Head of Service Delivery.

3.4. Need to know. The Need to Know principle essentially means that even if someone has the required clearance it does not mean they have automatic access to read data if it's not

necessary in order for that person to carry out their role. Staff will only be granted access to the data they need to carry out their duties.

3.5. Protection of personal data. Access to a computer system containing personal data files is to be restricted to authorised users. Our Data Security Policy specifies how users are authenticated and access is controlled. Personal data held on paper files is to be held in secure, lockable cabinets, with access to the keys restricted to authorised users only.

4. Data Protection Principles

4.1. Personal data shall be processed fairly and lawfully. Personal data held by DRCSAS will be processed for the following lawful purposes:

- by consent of the data subject;
- for the performance of a contract with the data subject or to take steps to enter into a contract;
- to protect the vital interests of a data subject or another person.

4.2. Personal data shall be used for the purposes stated at the time it is requested, and not for other purposes. Only personal data that is necessary for the purposes we have defined will be collected. We will ensure the data is sufficient for the purpose.

4.3. We will ensure the personal data we hold remains accurate. We will allow data subjects the opportunity to check and verify their personal data and the opportunity to submit changes or request deletions at any time. We will act on these changes immediately.

4.4. Personal data relating to employees past and present will be retained indefinitely in accordance with employment law and to enable accurate references to be provided. Personal data relating to our service users will be retained for 7 years to ensure service users don't have to repeat information if they return at a later date and to ensure data is available for public enquiries (e.g. domestic homicide reviews, Serious Case Reviews). Personal data on volunteers (including Trustees) will be held indefinitely to allow for references to made in future. Personal data on job applicants will be retained for 3 months.

4.5. We will keep this policy under review, specifically considering the reasons why we keep personal data and its retention period. Data subjects will be afforded access to their personal data on request. We will comply with requests from data subjects to amend or delete their data.

4.6. Personal data will be held securely with access limited to authorised users on a need to know basis. The security protection afforded to electronic and paper records is defined in our Data Security Policy.

4.7. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Notwithstanding, we will not knowingly transfer data to or use servers outside the UK.

5. Personal Data

5.1. Audit. A personal data audit is to be carried out annually to ensure we have full insight into the types of personal data we may hold about an individual. The audit is to record:

- The subject type;
- The data fields;
- The purpose for which it is required;
- The consent processes;

- The lawful means by which we may process it.

5.2. An analysis of how the data we collect is processed and stored is to be made and reviewed annually to ensure it reflects current usage.

6. Notices

6.1. Privacy notices. Privacy notices at the point of collection need to clearly indicate the purpose for which personal data is being collected and what it will be used for. The notice will clearly state how personal data may be shared, with data subjects given the option to opt in to sharing.

6.2. Individuals' rights. Individuals' rights will be stated clearly on the privacy notice: the right to access their data and how we can provide this data to them; their right to be forgotten (have their data deleted) and how we would delete their data; their right to correct any errors.

6.3. Consent forms. Consent forms will clearly state the range of data that may be collected, what it is used for, how it is processed and who it may be shared with. Data subjects will be given the option to agree to the sharing of personal data.

7. Data Handling and Data Sharing

7.1. Data security. Data is not to be shared or moved without proper authorisation. Data stored on our ICT system must not be shared unless there is a requirement to do so and authorised by the relevant manager. Guidance is provided to staff on the sharing of data.

7.2. Data is not to be moved or copied to other locations on our system where there is a risk it may be accessed by unauthorised users, or where it breaches the Need to Know principle. Documents are not to be left unattended where unauthorised users may access them.

7.3. When not in use, users are required to lock their computer or log out, even if the user will only be away for a short duration.

7.4. When not in use users are required to keep paper files in locked cabinets, and the user is to ensure the cabinet key remains safe. Faxes sent from/received at our copier, and documents scanned or printed, must be removed from the copier immediately and kept secure.

7.5. Data types. Due to the nature of our work, shared data concerning service users may include sensitive data. DRCSAS will not consent to sharing sensitive data about our employees past and present. Where sensitive data is shared we will ensure that explicit consent has been given (unless it can be demonstrated the data was shared in the vital interests of the data subject or another person).

7.6. Subject access requests. Data subjects may request access to the data we hold about them. The request may be made in writing or verbally. A record of all requests is to be made by sending the information to the Data Protection Officer. The appropriate worker must follow the Procedures for Processing Subject Access Requests within one month of the request.

7.7. Freedom of information requests. DRCSAS is not obliged to respond to freedom of information (FOI) requests. However, there may be contractual obligations to do this for certain projects, where the commissioner has included this in the contract terms and conditions. In such cases any requests must follow the terms and conditions laid out in the contract and must be restricted to data relating to the contract.

7.8. Receiving personal data. It is possible that DRCSAS will be sent personal data from another organisation. For service users, this data will normally relate to an individual who has given their consent for the data to be shared with us. In some cases, due to the nature

of the incident, consent may be implied. We will first check with the data subject that they are aware and consent to us acting on it. Further detail is contained in the Procedures for Processing Subject Access Requests.

7.9. Sending personal data. DRCSAS will only share personal data about service users with another organisation if the data subject gives their explicit consent or it can be demonstrated the data was shared in the vital interests of the data subject or another person (e.g. a safeguarding issue). In all cases data will only be shared if authorised by the Chief Executive Officer or Service Manager. The justification for sharing the data will be recorded in the case notes. Where possible signed consent will be obtained, but this is not essential. Further detail is contained in the Procedures for Processing Subject Access Requests. Personal data about staff members, volunteers or Trustees (e.g. for payroll and accountants purposes) will never be shared unprotected.

7.10. Security of data in transit. Data sent or received will be transmitted using our secure email system. Failing this the files will be password protected and sent by normal email. The password will be shared by another means, but never in the same email as the protected document.

7.11. Documents may only be printed on DRCSAS owned and operated printers within our secure offices.

8. Privacy Impact Assessments

8.1. Privacy impact assessments (PIA) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

8.2. New projects or services are required to conduct a PIA at the earliest stage of project development. The findings of the PIA are to be recorded and retained with the project documentation.

9. Data Breaches

9.1. If it is suspected that or there is evidence that a data breach has occurred the incident is to be reported to the Data Protection Officer (Chief Executive Officer), who is responsible for informing the Board of Trustees. The incident is to be investigated and action taken to stem the breach, inform those affected and learn and implement lessons to prevent future breaches.

9.2. Investigation. The investigation should cover as many of these as possible:

- When was the incident identified;
- How was it identified;
- Who identified it;
- What immediate steps were taken;
- If it was an ICT breach, follow the incident management section of the Data Security Policy;
- Who has been informed.

Appendix 1

Checklist

The checklist will help us decide if we are complying with the data protection principles. It will be incorporated into procedures and guidance for staff and volunteers.

Do I really need this information about an individual?	Y / N
Do I know what I'm using it for? (Lawful processing)	Y / N
Does the data subject know that I've got it?	Y / N
Will they understand what it will be used for?	Y / N
If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?	Y / N
Am I satisfied that the information is being held securely, whether it's on paper or on computer? What about my website? Is it secure?	Y / N
Is access to personal information limited to those with a strict need to know?	Y / N
Am I sure the personal information is accurate and up to date?	Y / N
Do I delete or destroy personal information as soon as I have no more need for it?	Y / N
Have I trained my staff in their duties and responsibilities under the Data Protection Act, and are they putting these into practice?	Y / N
Do I need to notify the Information Commissioner, and if so is my notification up to date?	Y / N

Policy Backing Sheet

Name of Policy: Data Protection Policy

Date Agreed by BoT: 09/04/2018

Date Amended	Date to be Reviewed
June 2024	June 2025