

Privacy Notices – Support Service

Safe Haven Sussex – Community Interest Company (CIC)

Name of Organisation:

Safe Haven Sussex CIC
The Dock Hub
Wilbury Villas
Brighton & Hove
BN3 6AH

Data Protection Officer:

Flora Papanicolaou-Hood: Director

1. Purpose of the processing:

To provide accommodation and intensive housing management support to single homeless individuals with support needs. To work with the individual and community services to ensure that the client is receiving holistic support in the community to encourage, recovery, attainment of skills and to move on to independence.

2. Lawful Basis:

(b) Contract: The processing is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract.

Special Category:

(h) Processing is necessary for the purpose of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment of the management of health or social care systems and services on the basis of Union Member State Law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

Criminal Offence Data:

The lawful basis to be used is (b) Contract – the same as above.

3. Why we collect your data:

We collect personal data for many reasons, including to provide you with services, to assess your individual support needs and to safeguard you and other service users you will be sharing accommodation with. Only if necessary for your individual support will we share information with relevant community partners. We will collect personal data to apply for housing benefit on your behalf.

We will collect personal data to enable the service to implement a comprehensive risk assessment and to write with you a personalised support plan to be able to work with you to achieve your short term and long term targets.

We will collect personal data to ensure that we are providing you with the most appropriate support in the community.

4. (a) Information we collect:

- Your full name
- Date of birth
- Contact details
- Details of previous and current housing arrangements
- Your bank details
- GP details
- Details of benefits that you have been awarded including but not only JSA, ESA or universal credits
- Any work details
- Educational information.
- Details of debts (if any)

(b) We will also collect sensitive personal information such as:

- Support needs, including the management of offending behaviour, alcohol or drugs. Health and Mental health needs, social needs including integration. Anti-social behaviours, Gang affiliations.
- Sexuality
- Ethnicity
- Criminal record

5. Who we will collect your data from:

- Community Support groups referring you to us
- You
- Probation office
- Police
- Social Workers
- Advocates
- GP's
- Mental health teams
- Local authority officers

6. How we collect data:

- Online referral form from referrers
- Face to face
- Email
- Telephone

7. How we keep data:

We will keep your case information including notes, letters and information given to us about you, in a confidential record that is specific to you. We use hard copy files that, when not in use are locked away in secure cabinets with keys only being available to relevant staff who need access to the information enabling them to support you most appropriately.

We run a clean desk policy, which means no private or sensitive information is left out when not in use.

We also use a customer relationship management system to support our guidance and support. This means that we can keep the information you or others provide us, so we are able to see the history and relevant details of your case. This ensures that we provide appropriate and accurate support. We take information security very seriously. No one is allowed access to our system or files unless they need this to provide the service to you or one of the other purposes described in this notice.

To ensure that our services meet a high standard of quality, clients files will be checked for quality assurance purposes.

We may use your data for statistical reports. These statistics will not include any information that could be used to identify any individual.

8. Security of your personal data:

We use appropriate technical and organisational measures and precautions to protect your personal data and to prevent loss, misuse or alteration of your personal data.

The transmission of information via the internet is not completely secure, although we do our best to protect your personal data, and we ensure as far as practicable any third party also use secure systems, we cannot always guarantee the security of your data submitted to our website. Once we receive your information we shall use strict features to ensure its security.

Staff are not permitted to take any sensitive data off site unless they are obliged to take to a meeting with officials you may have requested such information.

We will not use your data for any marketing purposes.

9. Who we share your data with:

We will not share your data with any third party unless it is vital to your care and support, or if we are obliged to for legal **and regulatory purposes**.

Therefore we may share your data with:

- Local Authority Offices such as Housing Benefit, DWP or any other department
- Probation offices
- Mental health teams
- Social services
- Community advocate groups
- Community support groups who may be supporting you with drug or alcohol problems
- Housing providers
- GP's
- Other health care professionals involved in your health care, including hospitals

10. Retention of your data:

Whatever your relationship with us, we will only store your information for a specified amount of time, as set out in our internal data retention policy.

The length of time that data will be kept may depend on the reasons for which we are processing the data and on the law or regulations that the information falls under, such as Health and Safety Regulations or any contractual obligations we might have such as with government contracts, or for research purposes, we will anonymise the data so no individual is identifiable.

Subject to the above, we will typically store data relating to service users who have left the service for 6 months.

Once the retention period has expired, the information will be confidentially disposed and or permanently deleted.

11. Your rights:

You have rights under the new GDPR, these include:

- **Right to access:** You have a right to ask for your personal data and supplementary information. This right allows you to be aware of and verify the lawfulness of the processing. You have the right to obtain:
 - Confirmation that your data is being processed
 - Access to your personal data; and
 - Other supplementary information as stated in the privacy notice above.
 - We will provide you with the information requested without delay and at the latest within one month of the request free of charge. However if we may charge a fee if your request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information.
- **Right to rectification:** You have a right to request for rectification verbally or in writing. We will make any agreed rectifications within a month of the request. In certain circumstances we can refuse to rectify under our obligations of the accuracy principle.
- **Right to erasure:** You have a right to have your data erased. The right to erasure known as ‘the right to be forgotten’
 - You can make a request for erasure verbally or in writing
 - We will respond to your request within one month of the request.
 - The right is not absolute and only applies in certain circumstances.
 - You have the right to have your individual personal data erased if:
 - the personal data is no longer necessary for the purpose which it was originally collected or processed for
 - if consent applies – it has been withdrawn
 - if there is a legitimate interest – you object to the processing of your data and there is no overriding legitimate interest to continue this processing
 - we are using your personal data for marketing purposes
 - we have processed your personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle)
 - we have to comply with a legal obligation
 - When does the right to erasure not apply? The right to erasure does not apply if processing is necessary for one of the following reasons:
 - To exercise the right of freedom of expression and information
 - To comply with a legal obligation

- For the performance of a task carried out in the public interest or in the exercise of official authority
 - For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
 - For the establishment, exercise of defence of legal claims.
- **Right to restrict processing:** You have a right to request the restriction or suppression of your personal data.
 - This is not an absolute right and only applies in certain circumstances. When processing is restricted we can store the personal data but will not use it.
 - You can make a request verbally or in writing
 - We will respond to your request within one month
 - This right has close links to the right to rectify.
 - When does the right to restrict processing apply?
 - You contest the accuracy of your personal data
 - The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and you oppose erasure and request restriction instead
 - We no longer need the personal data but you need us to keep it in order to establish exercise or defend a legal claim; or
 - You have objected to us processing your data under Article 21(1) and we are considering whether our legitimate grounds override yours.
 - We will not use the restricted data in anyway.
- **Right to data portability:** the right to data portability allows you to:
 - Obtain and reuse your personal data for your own purposes across different services
 - You can move, copy or transfer personal data easily from one IT environment to another in a safe and secure way without hindrance to usability.
- **Right to Object:** You have a right to object: You have the right to object to:
 - Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
 - Direct marketing
 - Processing for purposes of scientific/historic research and statistics
 - You must have an objection on “grounds relating to his or her particular situation”

- We will stop processing your data unless we can demonstrate compelling and legitimate grounds for the processing, which override your interests, rights and freedoms; or
- The processing is for the establishment, exercise or defence of legal claims.

12. Personal Data Breaches:

- a. We have a duty to report certain types of personal data breach to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.
- b. If the breach is likely to result in high risk of adversely affecting your rights and freedoms we will inform you without delay.
- c. We will ensure that we have a robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and you if you have been affected.
- d. We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

13. The Right to lodge a complaint: You have a right to lodge a complaint with the supervisory regulatory body. (ICO)

| | |
|--------------|---------------------------|
| Policy | Privacy Notice - Service |
| Created: | 24 th May 2018 |
| Review Date: | 24 th May 2021 |
| Created by: | Anna Constanti |