GREATERLONDONAUTHORITY

Rough Sleeping Services Data Protection and Information Sharing Policy

2022 -2025

DRAFT v1.3

Name of service	
Name of Service Provider	
Headline summary of the service and the purpose for which it collects and holds data	
Address of service	
Contact details for subject access requests and concerns re data breaches	
Email	
Postal address	
Telephone number	

In the policy below, the provider of the service will be called the Service Provider and the service will be called the Service Provided or the Service.

Contents

1. **Introduction and Purpose**
2. **Key Requirements**
3. **Definitions**
4. **Data protection management and notification**
5. **Responsibilities**
6. **How we ensure data is:**
    a. **Processed fairly and lawfully**
    b. **Processed for a specific purpose**
    c. **Adequate, and relevant but not excessive**
    d. **Accurate and up to date**
    e. **Retained no longer than necessary**
    f. **Processed in accordance with the rights of the data subject**
    g. **Subject to appropriate security measures**
    h. **Not transferred outside of the EEA unless there is adequate protection**
7. **Consent and exercising data subject rights**
8. **Data Sharing**
9. **Dealing with a breach of this policy**
10. **Review**

DRAFT

DRAFT

1. Introduction and Purpose

This is a policy for services:

- commissioned by the Greater London Authority (hereafter the GLA) that support people who are or have been rough sleeping,
- that are provided to prevent rough sleeping, and/or
- that support people with issues that intersect with rough sleeping.

There is a separate policy for CHAIN and Clearing House.

These services work with vulnerable adults and young people. The information they share enables the service to provide support tailored to the individual's needs.

The Service Provider collects and holds certain information on its clients and partners in order to successfully provide its service

The Service Provider is committed to ensuring that all personal data that it stores will be dealt with in line with the Data Protection Act 2018[1] and EU General Data Protection Regulation (GDPR). To comply with the law, personal information will only be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures used when delivering the service.

This policy covers the Service Provider, the service being provided, its managers, staff and volunteers.

As a matter of good practice, partner organisations and individuals working with the Service Provider, and who have access to personal information, will be expected to have read and comply with this policy.

2. Key Requirements

In line with the Data Protection Act 2018 principles, the Service Provider will ensure that personal data will:

- Be processed fairly and lawfully
- Be processed for a specific purpose
- Be adequate, and relevant but not excessive
- Be accurate and kept up to date
- Be retained no longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA) unless the country has adequate protection for the individual

3. Definitions

a. "personal data"

Personal data means data which relates to a living individual who can:

[1] http://www.legislation.gov.uk/ukpga/2018/29/contents

DRAFT

(a) be identified from that data, or

(b) be identified from that data and other information which is in the possession of, or is likely to come into the possession of, the Service Provider[2]

Personal data includes any expression of opinion about the individual and any indication of the intentions of the Service Provider or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held is still "personal data".

The definition also specifically includes opinions about the individual, or what is intended for them.

The following is a non-exhaustive list of the types of data that the Service Provider collects and holds which fall under the definition of personal data:

- Clients' personal information, including;
  - Unique identifiers (e.g. NINO)
  - Current address and housing history
  - Monitoring information (age, gender, etc.)
  - Support needs details
  - Contact details
  - Financial information (e.g. debts, benefits, etc.)
  - Details of other services involved in client support
  - Health details (physical and mental)
  - Offending history
  - Housing preferences
- Correspondence relating to support needs, referrals, nominations, transfer requests etc. (i.e. emails sent and received by Service Provider).

4. Data protection management and notification

The Service Provider will ensure that our details are registered with the Information Commissioner; we will notify and renew our notification on an annual basis. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

5. Responsibilities

Overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of the Service Provider this is the (Greater London Authority/ governing body of the Service Provider).

The governing body delegates tasks to the Service Provider. The Service Provider is responsible for:

- understanding and communicating obligations under the Act

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

DRAFT

- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes
- writing and regularly reviewing the data protection policy

All the Service Provider staff and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

6. How we ensure data is:

a) Processed fairly and lawfully

The Service Provider will be clear and open with individuals about the reasons for collecting, using and storing their personal data (as covered in section 6.b), and will seek consent to collect, use and store personal data for these purposes.

The Service Provider will not process personal data in a manner that causes unjustified detriment to the individual.

b) Processed for a specific purpose

The Service Provider obtains personal data for one or more of the following reasons; to:

- determine a client's eligibility for the service
- determine the service's suitability for a client
- understand a client's support needs so the service can be tailored to them, within the scope of the service
- ensure the safety of support staff lone-working with clients
- appropriately match clients with a property that meets their needs and preferences
- be shared with specific partner agencies for the purpose of informing their assessments or decisions
- be shared with specific partner agencies to ensure that appropriate client support is provided
- enable us to contact partner agency staff and notify them of decisions
- monitor the service and its effectiveness

The overall reason for the Service Provider to hold personal data on clients and their support workers is to enable to service to deliver on the outcomes and outputs agreed with the GLA for that service, which are part of the GLA's overall approach to supporting people to move off the streets and into stable accommodation.

c) Adequate, and relevant but not excessive

The Service Provider has a duty of care to its clients and partnership workers which requires us to collect sufficient personal data to ensure that appropriate decisions with regard to provision of services and support are made, and to ensure the safety and wellbeing of all involved. However, there is also a legal requirement for the Service Provider to not hold more information than is necessary for these purposes.

DRAFT

The Service Provider will not obtain personal data that is not considered relevant to the purposes of section 6.b and will regularly review the information that it collects to ensure this. Any irrelevant or excessive data provided to The Service Provider will be deleted.

d) Accurate and up to date

The Service Provider will take reasonable steps to ensure that the personal data that it holds is accurate and kept up to date.

Upon completion of a form providing personal data we will require clients and partnership workers to confirm that the information provided is accurate and complete.

Partnership workers will be given the facility to access the current records of their current clients in order to check that the information held is accurate. Workers will be encouraged to notify The Service Provider of any inaccurate or out of data information held and will be required to update and re-confirm the accuracy of existing data on a regular basis.

The Service Provider staff will check and query any information held that is believed to be inaccurate or out of date; this may be done via email or telephone conversations. Records of any information gathered in this manner will clearly indicate how it was obtained, by whom, from whom and when.

e) Retained no longer than necessary

The Service Provider will not retain personal data for any longer than is necessary in order to achieve its purpose. If it is identified that a piece of information is no longer required for any of the reasons given when it was collected, then this information will be deleted.

It should be noted that, as one of the reasons the Service Provider collects personal information is related to statistical reporting and monitoring of the service, data may often be held beyond the end of a client's direct involvement in one or more aspects of the service.

Where information is held by the Service Provider on an ongoing basis. The reasons for this are:

- There is a possibility of clients returning to the service, and in that event the records of the service previously provided would be required to effectively provide support.
- Whilst a client is in receipt of a service it will be necessary for their records to be kept in order to ensure the on-going provision of that service.
- Undertaking longitudinal analysis of pan London supported accommodation provision is essential to support the development of policies to alleviate homelessness for the GLA and other statutory agencies.

f) Processed in accordance with the rights of the data subject

This refers to the following rights:

- Right of access to a copy of the information comprised in their personal data
  This is referred to as a Subject Access Request. This right means that an individual may request and is entitled to be;

DRAFT

- told whether any personal data is being processed
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data; and given details of the source of the data
- See section 7 on Subject Access Requests for details about this process.

- Right to object to processing that is likely to cause or is causing damage or distress
  An individual has the right to object to the processing of their own personal data; they must do so in writing specifying why the data is causing unwarranted damage or distress. There are exemptions to this right, e.g. if the individual has consented to the processing of their data.

- Right to prevent processing for direct marketing
  The Service Provider will not contact the client for the purpose of direct marketing. Should they wish to do so in the future, for example to promote services, they will seek prior consent and comply with any client request to cease communication, in line with the Data Protection Act 2018. The GLA must be advised in advance of any plans to contact clients for the purposes of direct marketing and any direct marketing should be recorded in quarterly monitoring reports.

- Right to object to decisions being taken by automated means
  The Service Provider may use a custom database system and other electronic records which uses some automated processes, however these are only ever applied to support human decisions, and the decisions themselves are not taken by automated means.
  There are no plans for this to change, however, where it to change in the future The Service Provider would comply with the requirement to explain and/or reconsider this decision, as per the Act and will advise the GLA in advance of any such plans.

- Right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
  See section 6.d.
  If notified of inaccurate personal data, the Service Provider will correct or delete it as appropriate within a reasonable timeframe.

- Right to claim compensation for damages caused by a breach of the Act

g) Subject to appropriate security measures

For operational and technical reasons some data may be duplicated and stored on the Service Provider's own secure servers. The Service Provider will know where the servers are located and ensure that there is adequate protection including restricted access to the physical servers.

DRAFT

Appropriate technical measures such as secure connections and firewalls must be in place and kept up to date. The location of personal data saved to these servers must only be able to be accessed by an authorised member of the Service Provider team who would have to access the network using their individual network account which is password protected.

Some personal data held by the Service Provider is stored electronically.
The information held by the Service Provider must only be accessed by the Service Provider's staff employed for the purpose of delivering the service. In order to access the data staff must first log in to the secure Service Provider's system and/or network using their individual username and password.

The following safeguards should be observed:

- Access to the information systems of the Service Provider is granted to individuals because of the specific role they work in. Workers may only use the system or look up information on the system where it is of direct use in the role for which they were granted access. Use of the system will be monitored to ensure correct and appropriate use.

- Users must never share their log-ins, including their password, with any other person.

- Organisations using The Service Provider's service or delivering part of it on behalf of the service provider, should have policies and processes in place to ensure that staff access data securely. For example, The Service Provider's information/case recording system should not be accessed on a computer which may be visible to clients of a service, and caution should be exercised in using mobile technology in public places.

- Information should only be downloaded when necessary and where the file can be safely stored on a secure server. Downloaded data should be archived and destroyed in line with organisations' individual policies.

The Service Provider aims to have a culture of security awareness. Staff will receive the appropriate training in this area and understand the importance of data security.

h) Not transferred outside of the EEA unless there is adequate protection

The Service Provider will not transfer personal data outside of the EU. The possible exception to this is where data is stored, or certain platforms (e.g. For Clearing House via the Salesforce platform, in data centres in the United States of America. It should be noted that the data is not shared with or accessed by any partners in the US, it is only stored or transferred through the US).

For the record, and as an example, Salesforce adheres to the US-EU Safe Harbour Framework[3] which is considered to constitute adequate protection under the Data Protection Act 2018.

7. Consent and exercising data subject rights

User Agreement

[3] http://www.salesforce.com/uk/company/privacy/full_privacy.jsp

The member of staff in a commissioned service will sign up to a user agreement when accepting a login for the Service Provider's system. These will outline the terms within which the worker will operate, including the handling of data. Any breach of these terms will result in the access to the system being removed.

(a) Client consent
Consent should be obtained before someone's personal information is put onto the Service Provider's information and recording system. When completing referral forms, workers will be requested to confirm that the client agrees to the referral and information in it to be submitted.

(b) Clients who refuse to give consent
If consent has not been secured, information can still be processed if it is in the legitimate interests of the data controller or the organisation adding information. There are times when information, including personal, sensitive information needs to be recorded on the Service Provider's information and record keeping systems without consent being given. It is important to record instances where consent was refused. Please see 4.2 below about clients' right to request that possessing of data ceases.

(c) Clients who withdraw consent at a later date
This will be considered under the amending or deleting data procedure below.

Subject Access Request
Under the Data Protection Act 2018, individuals have the right to access the personal data that the Service Provider holds about them. Anyone wishing to exercise this right should apply in writing to
the manager at the Service Provider by email or post to the addresses at the top of this document.

A Subject Access request may be for any or all of the following:

- to be told whether any personal data is being processed;
- to be given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- to be given a copy of the information comprising the data; and given details of the source of the data (where this is available)

If a specific piece of data is being sought this should be clearly stated. You will also be asked how you would prefer to receive the results of your request; in most cases an electronic copy is most appropriate.

Before a Subject Access Request is considered to have been received you will be required to provide proof of identification, in the form of a passport or similar document.

Once the Service Provider has received all of the above we will seek to comply with the request as soon as possible and within the required 40 days from when all documents are received.

Amending or deleting data
Clients have the right to request to have inaccurate personal data removed or corrected. If someone views their data or is told by a worker about some information held by the Service Provider that is incorrect, for example on the case management system, they can request this is corrected or removed. This request should be sent to the Service Provider team to be logged at the details given at the top of this document. The Service Provider's team will ask

DRAFT

an appropriate manager to investigate whether information is inaccurate, and action will be taken accordingly.
An individual has the right to object to processing that is likely to “cause substantial damage or distress”. In certain circumstances the processing of personal information may still continue when a client claims that it is causing them damage or distress because it is in the partnership workers’ legitimate interests.

If someone has asked for all their data to be removed from the system, a short investigation about why this has been requested will be undertaken by the Service Provider’s team and the main partnership workers in relation to the record (i.e. current or recent support workers). In some cases it will not be possible to remove a record from the Service Provider’s information and case management system or other records, as information is required to provide services and to help to support the individual to address their homelessness and support needs. The decision about removing or retaining a record will be made through consensus between the main partnership worker(s) and the Service Provider’s management. In the case of a satisfactory decision not being reached, the GLA will make the final decision on the best course of action to take. By adding data to the Service Provider’s information systems, organisations agree that this information will be shared and that decisions about removing information will be made in conjunction with the relevant parties, including the Service Provider and the GLA who have final decision-making authority.

Complaint
Clients should be able to make a complaint about workers recording information, or any other aspects of the service offered to them, by following individual organisations’ complaints processes. They may also choose to make a complaint to the Service Provider about the Service Provider team and they can also contact the Information Commission if their complaint is specific to data recording.

8. Data Sharing

Data sharing may form an essential part of the work of the Service Provider, especially where the role involves liaison between other service providers. Data sharing is essential to the way in which some support services for rough sleepers and former rough sleepers operate. Without it, the support could not be delivered.

The Service Provider should seek clients’ consent to share necessary personal data at the point that their referral form containing said information is submitted to us. If consent is withheld or refused at this point, the client's data will not be shared with any partners, unless emergency exceptions apply. However, this will mean the Service Provider will not be able to provide its service to the client in question and the consequences of this need to be raised with the relevant agencies, as appropriate, in a timely manner.

When completing a referral form, there is a degree of information sharing provided between referral agencies by default, however this is limited within each organisation with which the Service Provider partners.

Sharing information from the Service Provider
Information from the Service Provider’s system should not be shared with a worker or agency that cannot view or access that information for themselves. The Service Provider should be contacted for advice if there are any doubts or concerns about information sharing.

DRAFT

Exceptional information sharing (outside of systematic data sharing for the agreed purpose of the service) such as to the police will only be agreed where a clear case is made involving the safety of the client or another individual or a serious crime, and the information cannot be obtained from other sources.

This is because of the consent clients give – for information to be shared to benefit them in terms of service provision.

When the police request information, the Service Provider's team asks for a DPA form and a manager assesses the request on this basis and decides whether to refer the police to that service.

Service Providers do not generally respond to missing persons enquiries. This is not the purpose of the system. A search for information may be undertaken if there is there is a serious and immediate concern about the person.

9. **Dealing with a breach of this agreement**

If any user becomes aware of any misuse of the Service Provider's information they should inform the Service Provider team immediately. This includes any loss or unauthorised disclosure of personal data, damage or loss due to malicious software/hacking or disclosure to a person not entitled to receive information.

The Service Provider team will follow up any reports of a breach of this policy and the GLA will be informed immediately. Initially those involved will be consulted by a manager from the Service Provider team with a view to achieving a resolution that is acceptable to all concerned. If a reported breach is substantiated and deemed serious and significant by the GLA, the project or organisation concerned may have their access to the Service Provider revoked.

10. Review

This policy will be reviewed every 3 years or when there is a significant change in the service, whichever comes first.

DRAFT