MAYOR OF LONDON

Greater London Authority Rough Sleeper Services Information Sharing Protocol

Version	**3.0**
Author	Martin White
Date created	18/07/2011 (v1)
Date reviewed	01/03/2014 (v2)
Reviewed by	Lisa Luhman
Date reviewed	01/07/2015 (v3)
Reviewed by	Jonathan Qureshi

1 Introduction

1.1 The purpose of this protocol is to outline the legal terms and conditions which apply to the management and sharing of personal information by all services commissioned by the Greater London Authority through the Housing and Homelessness Unit's Rough Sleeping Team. This protocol covers all the data held by or on behalf of the GLA. It includes, but is not restricted to, data held on CHAIN and any other databases. It aims to create a common set of standards, processes and expectations between all signatories to the protocol with regard to data and information sharing.

1.2 There are two main sorts of information sharing: systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and one-off decisions to share data for any of a range of purposes.

1.3 The content of this protocol is relevant to both types of information sharing.

1.4 The scope of this protocol is to clarify as far as possible, under which circumstances information can be exchanged. The intention is that a single, joint approach to exchanging information will be the most efficient mechanism for joint working regarding the delivery of services for rough sleepers.

1.5 It is intended this protocol will be a *live* document as the content contained within it will always be susceptible to changes in the law and best practice and need to be updated and amended regularly. This protocol will assist all staff members in rough sleeper services by enabling them to be aware of the relevant issues before deciding to share information. It also aims to encourage a significant level of standardisation in the exchange of information.

1.6 This protocol is due to be reviewed in July 2016 unless substantive legislative change occurs or repeated operational issues arise around the application of this protocol.

1.7 This protocol should be read in conjunction with the Information Commissioner's Data Sharing Code of practice https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

2 Benefits of Information Sharing

2.1 The secure and appropriate transfer of confidential information is a vital part of an effective support system. It is essential to promote partnership working, joint planning and an integrated service offer for rough sleepers.

2.2 For individual clients whose data is shared this should lead to an improved service offer being available to them through better communication between the agencies involved in their support.

2.3 For the wider community, data sharing will help services maximise their effectiveness and commissioners to better understand rough sleeping needs and commission services to address these needs thereby reducing the amount of rough sleeping and the associated wider social impacts that this causes.

3 Risks of not sharing information

3.1 If information is not managed appropriately between relevant providers it can have a negative impact on service delivery. However, as providers work more closely together to develop an integrated service offer, there is the potential to threaten the privacy and confidentiality of the individual, particularly as information technology is more widely used.

3.2 It is therefore vital that all commissioned services demonstrate a commitment to share information responsibly, appropriately and securely. They must establish open, transparent and accountable procedures and agreements that manage the exchange of information to aid service delivery whilst keeping personal information protected throughout.

3.3 However, in all cases where information sharing is being considered the following factors shall be referred to:

- What is the sharing meant to achieve?
- What information needs to be shared - i.e. not all the personal data held about someone should be shared if only certain data items are needed to achieve the objectives of data sharing?
- Who requires access to the shared personal data – 'need to know' principles should be applied, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data?
- When should it be shared – i.e. is the data sharing meant to be routine, one off or in response to specific events.
- How should it be shared – i.e. what is the most secure method the data can be shared?
- Is the data sharing achieving its objectives?
- What risk does the data sharing pose?
- Could the objective be achieved without sharing the data or by anonymising it?

4 Types of information that will be shared and the purposes that it might be shared for

4.1 The information disclosures may consist of:

1. Personal client information as identified during assessment and case work between service providers. Personal data applies to any information by which an individual can be identified (for example, but not limited to: name, address or date of birth).
2. Sensitive personal data as identified during assessment and case work between service providers. Sensitive personal data consists of information relating to:
    a. Racial or ethnic origin
    b. Political opinions
    c. Religious beliefs or similar
    d. Trade union membership (Within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
    e. Mental or physical health conditions – this would include needs around drug or alcohol misuse as well as details of physical or mental health conditions.
    f. Sexual activity
    g. The commission or alleged commission of any offence

h. Any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.

3. Client medical information as identified during assessment and case work between agencies
4. Any other information recorded on the CHAIN database system.

4.2 Specifically information will be shared for the following purposes:

1. To promote the health and well-being of service users.
2. To reduce the risks of associated with rough sleeping to individuals and the community.
3. To promote improved partnership working and integrated service offers between service providers.
4. To support risk management procedures.
5. To ensure that data is managed effectively and in accordance with legal responsibilities of staff members and organisations.
6. To enable analysis of the performance of individual providers and the groups of providers, including tracking outcomes for service users.
7. The protection of children, young people and vulnerable adults.
8. To undertake research and audit.

5 The Role and Responsibility of Partners

5.1 Signatories to this protocol are obliged to share information in accordance with the standards set out in this protocol.

5.2 This Information Sharing Protocol has been approved by the GLA's Information Governance Manager.

5.3 The management of the risks and benefits of information sharing as a result of this protocol will be governed and overseen by GLA's Rough Sleeping Commissioning team

5.4 Each service provider signed up to this protocol will nominate a senior manager to act as Information Asset Owner who will have the responsibility for ensuring that this protocol underpins the practical application of partnership working and all staff are made aware of this protocol, understand its principles and are able to use it effectively.

5.5 Each service provider signed up to this protocol will ensure that the parameters of information sharing will be fully explained to every service user during initial assessment or, if it is not in the service user's interests for this to be done at this time, then at the first possible opportunity thereafter. This will include the service user's right to confidentiality and the reasons why this confidentiality might be broken. Service providers will apply the same standards to information about deceased people as they do to information about living people.

5.6 Each service provider receiving data from another partner will not use it for any other purpose than is set out in this protocol, nor share it with any other party, without the disclosing partner's written permission.

5.7 Each service provider will ensure that all third parties affiliated to them will comply with the standards in this protocol.

5.8 Any service provider may withdraw from this protocol upon giving written notice to the GLA and the other partner signatories. Data which is no longer relevant should be destroyed or returned. The

service provider must continue to comply with the terms of this protocol in respect of any data that the partner has obtained through being a signatory.

6 Legislation

6.1 The manner in which information can be exchanged will take into account the following legislation and policy requirements:

1. The statutory right of the organisations to share information
2. The Human Rights Act – Article 8
3. The Data Protection Act 1998
4. Common Law Duty of Confidence
5. The Freedom of Information Act 2000
6. Disability Discrimination Act 1995 (as amended 2010)
7. Copyright, Patents and Design Act 1988
8. Computer Misuse Act 1990

6.2 Each service provider pledges to check and update the relevant systems (i.e. CHAIN, case management systems) and paperwork to ensure that it is appropriately registered for sharing and receiving personal information for the purposes of this protocol.

6.3 The data controller determines the purposes for which and the manner in which any personal data are to be processed. For the purposes of this protocol the GLA is the data controller.

6.4 The data controller must ensure that any processing of personal data for which they are responsible complies with the Data Protection Act 1998.

6.5 The relevant grounds for legitimate processing of any personal data according to Schedule 2 of the Data Protection Act 1998 are:

1. The data subject has given consent for the processing.
2. Processing is necessary for the performance of, or commencement of, a contract.
3. Processing is necessary for compliance with any legal obligation other than an obligation imposed by contract.
4. Processing is necessary to protect the vital interests of the data subject.
5. Processing is necessary to carry out a public function.
6. Processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the data subject).

6.6 It should be noted that the data subject's vital interests are usually only considered to relate to matters of life or death.

6.7 Where consent for data sharing has not been given signatories to this protocol will be acting under Schedule 2 (Paragraph 6) of the Data Protection Act 1998 which allows processing necessary for the purposes of the legitimate interests of the data controller or third parties when balanced against the rights and freedoms of the data subject.

6.8 The relevant grounds for legitimate processing of sensitive data are:

1. The individual who the sensitive personal data is about has given explicit consent to the processing.
2. The processing is necessary so that the organisation complies with employment law.

3. The processing is necessary to protect the vital interests of: - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or - another person (in a case where the individual's consent has been unreasonably withheld).
4. The processing is carried out by a not for profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
5. The individual has deliberately made the information public.
6. The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
7. The processing is necessary for administering justice, or for exercising statutory or governmental functions.
8. The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
9. The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.
10. The processing is in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

6.9 Where explicit consent for data sharing has not been obtained, under paragraph 10 of Schedule 3, the Data Protection (Processing of Sensitive Personal Data) Order 2000 No. 417 permits the processing of sensitive personal where it :

4
(a) is in the substantial public interest;
(b) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and
(c) is carried out without the explicit consent of the data subject because the processing –
(i) is necessary in a case where consent cannot be given by the data subject,
(ii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or
(iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

Signatories to this protocol must satisfy themselves that the necessary legal requirements for sharing have been met.

7 Consent and Information Sharing

7.1 Every service provider must be able to evidence that consent underpins every aspect of information disclosure unless in cases where the justification for processing information meets the criteria of Schedule 2 and/or 3 of the Data Protection Act 1998. (Please see sections 6.5-6.9).

7.2 All service providers will ensure that every service user is aware of their right to confidentiality and will not share personal information without the informed, fair and freely given consent of the service user involved, unless in cases where the justification for processing information meets the criteria of Schedule 2 and/or 3 of the Data Protection Act 1998. (Please see sections 6.5-6.9).

7.3 At the point of initial assessment, the nature of personal information which will be collected and disclosed to other partners will be fully explained to the service user including why it is being collected, how it will be stored and who it is being shared with. This ensures personal information is

processed fairly and lawfully and the process is open and transparent in line with the Data Protection Act 1998.

7.4 Incapacity to consent must be judged on an individual basis and service users who have mental health difficulties or who present as intoxicated or confused, for example, still have a right to confidentiality.

7.5 It is acknowledged that there may be certain situations where professional judgement is made without obtaining consent where it is possible the privacy rights of the individual may be compromised.

7.6 In these instances a risk assessment will be undertaken weighing the responsibilities of the service provider and the interest of the public against the individual's right to privacy as outlined in the Human Rights Act 1998 to ensure the disclosure is fully justified. If the disclosure of information will in some way restrict the rights of the service user, service providers will also consider a test of proportionality. This is to ensure that a fair balance must be achieved between the protection of the individual's rights with the general interests of society, in accordance with points 6.7 and 6.9.

7.7 The situations where risk assessments and proportionality decisions may be required could include, but not be limited to, situations where the service user is in a mental or physical state that prevents them from providing consent and:

- the service user requires urgent medical treatment;
- the service user is at risk of significant harm or harming someone else;
- information sharing is necessary in order to protect children, young people or vulnerable adults from abuse or neglect;
- Information sharing prevents the service user from committing a criminal offence that could place others at risk or places the member of staff or others at risk of collusion;
- information is requested by the Police or other law enforcement agency for the purpose of the prevention or detection of crime or the apprehension or prosecution of offenders; or

7.8 These risk assessment and proportionality tests must be made at an Information Asset Owner level and the justification for disclosing personal information from the service user without obtaining consent must be clearly recorded in the service user's case file including the evidence or information on which the decision is based. This must include details of any third parties and full details of the information which has been shared.

8 Information Exchanges

8.1 The partners sharing information should be fully aware of the laws affecting the use of personally identifiable information and will comply with their requirements. Each service provider undertakes to ensure that it complies with all relevant legislation, this protocol and its internal policies on disclosure.

8.2 When disclosing personal information, parties to this protocol will state clearly whether the information being supplied is factual, an opinion or a combination of the two.

8.3 Service providers will apply the following principles at all times in the exchange of information. These are:

- To justify the purpose for which the information is to be exchanged
- Not to use personal information unless it is absolutely necessary
- To use the minimum amount of personal information necessary
- Access to personal client information should be on a strict need-to-know basis

- That everyone handling data should be aware of their responsibilities and must understand and comply with the law.

8.4 Each service provider must ensure the information they exchange is as accurate and as up to date as possible.

8.5 Parties to this protocol agree that where possible and appropriate, information requested in the correct manner as agreed between partners is given in a prompt and timely manner.

8.6 All requests for information to be shared or exchanged will be specific to the purpose, recorded in the service user's case file and on a need to know basis.

8.7 All information exchanged will be adequate, relevant and not excessive in relation to the purposes for which it is processed.

8.8 Service providers must use information only for the purpose for which it is requested, securely store it and destroy it when no longer required.

8.9 Where staff members are not sure whether to share information they should seek the advice of the Information Asset Owner of their organisation.

8.10 Each service provider must ensure that all staff involved in exchanging and collection of personal information within the drug treatment system are made aware of this protocol, understand its principles and are supported to be able to apply its principles effectively.

8.11 It is expected that all service providers signed up to this protocol work within standard and agreed formats for data entry and storage.

9 Security and Data Management

9.1 Parties to this protocol will ensure they have adequate security arrangements and measures in place in order to protect, store and transmit the information it processes in order to ensure the confidentiality, integrity and availability of the information held and disclosed. Personal information disclosed or held must:

- Be transmitted securely
- Be protected by back up rules
- When stored on a computer system, this must be access protected with this access reviewed regularly
- When manually stored, be stored in a secure locked filing cabinet within a lockable room when not in use
- Be located in a geographically secure environment

9.2 Service users have the right to access the personal information held on their file. Each partner should have a procedure on how it will satisfy Service user access rights within 40 days of the Service user access request being received.

10 Complaints

10.1 Each service provider is expected to have a procedure for managing complaints from service users. Any formal complaint by a service user regarding any stage of this information sharing protocol

should be resolved in accordance with the organisation's internal complaints policy. The partner's response and actions regarding this complaint should then be communicated in writing to the GLA's Rough Sleeping Services and Commissioning Manager and the all other partners as a best practice measure.

10.2 External complaints or instances of non-compliance by a partner organisation are to be reported to the GLA's Services and Commissioning Manager.

11 Awareness Raising and Training

11.1 Each service provider must be able to evidence that all staff members involved in the workings of this protocol receive training on Information Governance and Data Protection and be supported to apply this to their daily practice. It is, however, the responsibility of the staff member to ensure service users understand the concept of confidentiality.

12 Breaches

12.1 Any breach of confidentiality will seriously undermine and affect the credibility of the partners to this protocol and is liable for breach of the law. Any breaches of this protocol are to be investigated and resolved by the relevant Information Asset Owner and / or senior management within the particular organisation and the findings communicated to GLA.

13 Monitoring and Audit

13.1 The application of this protocol will be monitored by the GLA's Rough Sleeping Services and Commissioning Manager or Commissioning Project Officer through quarterly monitoring meetings and regular internal and external audit. Partners will be required to provide information to evidence their compliance with this protocol.

14 Freedom of Information

14.1 This protocol is not confidential and will be available for anyone to view

Signatories Section
On behalf of GLA…….
Service and Commissioning Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...
Service Manager
On Behalf of Organisation……...

Service Manager