DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	**Rough Sleeper Outreach MDT pilot (final name tbc)**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Chris Lehman – Head of ASC Strategy & Commissioning
	IAO name and asset	
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acronyms on first use.*	The Rough Sleeper multi-disciplinary team (MDT) outreach pilot will test out an MDT outreach way of working with rough sleepers with complex needs in Camden, with the aim of increasing access to mental and physical healthcare and substance misuse support needs. The pilot funds a new outreach Nurse (provided by UCLH), Psychologist post (provided by Camden & Islington NHS Trust) and Mental Health Worker (provided by Likewise), with peer support (provided by Groundswell) who will respond to referrals made by LB Camden's commissioned CGL outreach service staff, and meet clients within the community namely at the RTS hub or street sites. Overview of project: (please find referral pathway & very draft data sharing doc attached) • A new 12-month funded service to pilot an outreach-based multi-disciplinary team (MDT) approach to working with rough sleepers with complex needs • A service commissioned in a different way to increase access to mental and physical healthcare, and substance misuse services • A new outreach Nurse, Psychologist and Mental Health worker will work closely with Camden's commissioned outreach service (CGL) to identify rough sleepers requiring a coordinated and outreach response; there will also be close working with Inroads substance	

	misuse outreach (Westminster Drug Project), along with peer support services • MDT coordinated care is widely seen as best practice in providing health and social care to homeless people and is recommended in NICE guidelines for this cohort Data sharing/ single outcomes record • Effective MDT and coordinated care will depend on the main agencies ability to share information • It would be preferable to have a single database to collect MDT outcomes under unique identifiers (name of client) potentially via the CGL CRiiS system if possible • Continuation / mainstreaming of these much-needed posts will require evidence of impact data Urgency of timelines: • There is potential for some elements of the service to start early, with full-time posts in place by end of April
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	The service is anticipated to commence at the end of April 2023, although some elements of the service may commence sooner than the official start date (e.g. a day a week for the outreach nurse – this is still being decided)

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	No
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	No
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	No
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	No
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	No
1.6	Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	Yes
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	No
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes -
1.9	Will data be combined, compared or matched from multiple sources?	Yes
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	No
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	No
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	No
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	No
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	Yes
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

Step 2: What personal data is being used?										
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						Change			
							New and changed			
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate									
	Personal Data									
	Name	Yes	Date of Birth	Yes	Gender	Yes	National Insurance Number		Financial Information about the person	
	Address	Yes	Email address	Yes	Telephone number	Yes	NHS No	Yes	Other eg a reference number such as Mosaic ref	Yes
	Other data *(Please state)*:									
	Special Categories of Personal Data									
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					
	Trade Union membership		Physical or mental health or condition							Yes
	Sexual life or sexual orientation	Yes	Housing records Social services records	Yes	Tax, benefit or pension records		Employee/HR records			
	Other data *(Please state)*:	Not housing records, but accommodation status will probably need to be shared – i.e. 'street homeless/ Emergency Shelter/ TA								
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Yes Where this relates to risk assessment								

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared? Please use plain English!**	Referrals from outreach teams with high level information about the client will be made to the outreach nurse, psychologist, mental health support worker, Westminster Drug Project (substance misuse outreach team) and in a briefer form, to a peer support charity. Information between the nurse, psychologist, mental health support worker and substance misuse workers and most likely to GP practises about health outcomes - , where these are relevant to the other party - in order to effectively coordinate care around the person, may be shared via nhs.net email (I'm currently checking if the substance misuse outreach use these). Support needs may also be discussed between providers
3.2	**Explain in as much detail as possible why this is being done**	• To effectively coordinate services around a person with complex needs, to ensure that co-existing health support needs are treated in parallel, and in particular to help overcome well documented barriers to access between mental health and substance misuse services • To increase access to statutory health services on an outreach basis for rough sleepers who have complex needs and do not engage well with mainstream services due to stigma, often chaotic lifestyles, and effects of childhood trauma among other factors. • Providing a pre-treatment offer, moving people from a pre-contemplative phase to an action phase supported by peer workers with lived experience of rough sleeping, and a joint physical and mental health approach to outreach. • Supporting the wider development of rough sleeping services to better manage this cohort, for example being trauma-informed and managing complex overlapping needs.

<table>
<tr><td></td><td colspan="2"></td><td>

- Reduced crises and hospital admissions, alleviating pressure over the winter period
- To gain a clearer picture of mental and physical health needs of rough sleepers in Camden in order to commission the right targeted services going forward
- Increasing collaboration btw homeless outreach and health providers

</td></tr>
<tr><td rowspan="5">3.3</td><td colspan="2">Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td>Yes with CGL, C&I, Likewise and WDP.

It may be that individual activity / outcomes data is shared from each provider to the council, before this is sent on to NHSE for their funding purposes.</td></tr>
<tr><td>External organisation or partner Name</td><td>Controller or Processor?</td><td>Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? Yes/No/In progress</td></tr>
<tr><td>LB Camden</td><td>Controller –</td><td>In progress</td></tr>
<tr><td>Change, Grow, Live (CGL) (not being directly funded by this pilots funding but will require close working)</td><td>Controller</td><td>Yes</td></tr>
<tr><td>ULCH Hospital Trust</td><td>Controller</td><td>In progress</td></tr>
<tr><td></td><td>Camden & Islington NHS Trust (C&I)</td><td>Controller</td><td>In progress</td></tr>
<tr><td></td><td>Westminster Drug Project (not being directly funded by this pilots funding but will require close working)</td><td>Controller</td><td>In progress</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>3.4.</td><td colspan="2">Please explain your process from start to finish. you can do this is a diagram if you wish, or a flow chart, or describe it. You can attach a document if that's easier.</td><td>Please see attached document</td></tr>
<tr><td>3.5</td><td colspan="2">How will you handle data in your project, how will use store and share it. Please explain</td><td>Health data will be kept and stored on health providers individual casework systems, i.e. Rio2 for C&I, EPIC for UCLH. However, activity and some health information may be kept on a central casework system on the CGL CRiiS database system, which could potentially provide access for other agencies to input into;</td></tr>
</table>

		this option is currently being explored, and we would like DPOs advice on this aspect.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify the Lawful Basis for processing personal data/special category /criminal data.** **If you don't know then please ask Data Protection Advice Team for advice (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition Article 6(1)(c) legal obligation and art 6(1)(e) public task.	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Art 9(2)(b) Employment, social security and social protection with the Data Protection Act 2018 Schedule 1 part 1 condition being para 2 health or social care purposes, and DPA18 schedule condition Art 9(2) (g) Reasons of substantial public interest with the Data Protection Act 2018 Schedule 2 Part 2 conditions being para 6 Statutory and government purposes, and para 18 Safeguarding of children and individuals at risk, with the underlying laws for both being Children Acts, Care Act, Health and Safety at Work etc Act 1974 and Localism Act 2011; and 9(2) (h) Health or social care with the Data Protection Act 2018 Schedule 1 part 1 condition being para 1 employment, social security and social protection, and para 2 (2) (d) the provision of health care or treatment; and 9(2)(e) the provision of social care, with the underlying law being Children Acts, Care Act, Health and Safety at Work etc Act 1974 and Localism Act 2011	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Criminal offence data- article 10 is met by the art 6 conditions as for personal data, and the DPA18 schedule conditions as for art 9 for special category data

4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Data Protection Advice Team have advised this is appropriate**	
	CGL will seek consent from someone at the point of initial assessment for treatment and referral; that said there may be circumstances where a person is not engaging, but the outreach team believe would strongly benefit from a nurse visiting their sleep site to talk to them. In data protection terms consent is not the legal basis	
4.3	**How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below	
	Through the use of pre-written referral forms and guidelines on data sharing within MDT meetings	
4.4	**Have/ will individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Privacy Notice? Remember telling people is not the same as asking for consent	Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes; in contracts and DSAs as necessary	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject.	
	No	
4.7	**Data Retention Period - how long will the data be kept? What will happen to the data at the end of the project – deleted or kept? If you're using a processor what are the arrangements with them for data at the end of the project?**	
	MDT information will be kept for the life of the pilot only. Health records on individual statutory health providers will be party to their own data rules on this.	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, SharePoint, shared drives,*
	Rio2 casework system – C&I EPIC casework system – UCLH CRiiS casework system – CGL – potentially storing high level casework and outcomes between providers Likewise casework data system Data may need to be sent to the council for analysis / collation / to clean data in order to send outcomes information and activity reporting to the main grant funders (NHSE)
5.2	**In what country is the data stored?**
	The UK
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Outreach nurse role Psychologist role Mental health support role Inroads substance misuse worker (tbc) Outreach key worker – in terms of high level referral No more information than is actually required will be sent through, which will be made explicit within any data sharing agreement
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	If one joint system is used to record outcomes/ service (i.e. the CRiiS system), then the data inputters require a log in, training and induction in order to access the system. Therefore, only very limited access to the system restricted to password-encrypted individual access.
5.5	**Is there an ability to audit access to the information?**
	As per the above
5.6	**What security and audit measures will there be to make sure that data is kept safe?**
	Depending on what was agreed, this would need to be informed by CGL should the CRiiS system be used as main outcomes database. However they are a commissioned service, so their database will comply with strict data safety rules.

5.7	Has the Information Security Team advised on the security measures? What were their comments?
	No.

Step 6: Identify and Assess Risks

Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Misuse of data; Personal data could be used in a manner incompatible with the Data Sharing Agreement. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.	Likely	Major	High
Data errors may not be checked and corrected by teams leading to inaccurate or unreliable data.	Likely	Moderate	Medium/high
CGL or providers accessing and sharing data inappropriately or using for unauthorised purposes	Likely	Major	High
Parties retaining data for longer than retention periods	Likely	Moderate	Medium/high
CGL or providers using data for unauthorised purposes	Likely	Major	High
The Criis system is insecure leading to a data breach	Likely	Major	High

Step 7: Identify Measures to reduce risk				
Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.* Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by /DPO* The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.				
Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Misuse of data	With professionals only log ins and effective role based access control the potential for this is very low as data inputters will be easily identified. All employees are covered by codes of contacts and are effectively vetted before appointment.	Reduced	Low	yes
Data errors.	CGL will provide appropriate training to a lead inputter from providers, which will be included in the new roles induction plan. CGL will also have a resourced database lead to maintain and check data and pick up on any anomalies. Data will be reviewed regularly at MDT meetings between providers to check for accuracy	Reduced	Medium	Yes
CGL or providers accessing and sharing data inappropriately	With professionals only log ins and effective role based access control the potential for this is very low as data inputters will be easily identified. All employees are covered by codes of contacts and are effectively vetted before appointment. No financial information is being collected reducing the risk of financial gain by misappropriation of data	Reduced	Low	Yes
Retaining after retention period	Each party has a defined retention period.	Reduced	Low	Yes

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				
[redacted]				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	Sarah Laws, Data Protection Manager
DPO advice	Approved, Andrew Maughan, DPO and Borough Solicitor, April 2023
Information Asset Owner acceptance of residual risks	Chris Lehman
This DPIA will kept under review by: (*usually the author or the IAO)*	[redacted]

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Willful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

IMPACT	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Table 4: is the risk level acceptable?

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) The Data Charter is here: Camden's Data Charter - Camden Council

1. *Effects on Residents*

a) *How does use of this data benefit our residents? (Is there evidence of this approach being likely to meet a public need?)*

- The sharing of information / data will improve the health of people most in need of a coordinated health intervention

b) *What would be the harm in not processing this data?*

- That an already social excluded cohort of societies health continues to worsen

2. *Data Bias*

a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?*

- There will need to be some dedicated admin time to review errors, duplications etc and clean data; this will be less of a risk if one system is used to collect

b) *Once errors and biases have been identified in data collections, how will they be taken into account for any future policy or service which uses this work as an evidence base?*

-

c) *Who could be negatively affected by processing this data?* (How can you show there is a **fair balance** between the **rights of individuals** and the **interests of the community**?

3. *Limitations of Data*

a) *How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?*

- The activity/ outcomes main database will only ask for data that is relevant for the evaluation / impact assessment of the service

b) *How are you ensuring the data used is reliable? (**Data quality**)*

i) *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

- Resource for collating and cleansing data will be identified

ii) *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**) (Are all metadata and field names clearly understood)*

- Yes

d) *How could the objectives of this project be completed without processing the data?*

- I don't think the objectives around system change and MDT working would be fully met without processing the data required.