Data Protection Impact Assessment (DPIA) - Full Assessment

Guidance for the Project Manager and Sponsor

The Data Privacy Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the people whose data you are dealing with. This template has been designed to incorporate the legal requirements of the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018 and in anticipation of the Data Protection Act 2018 becoming law. Data processing activities which started before 25 May 2018 and are continuing beyond this date should be assessed using this template if the conclusion of the pre-screening questionnaire is that the processing is high risk.

- The DPIA is a proactive approach to privacy protection;
- It is often the most effective way to demonstrate to the Information Commissioner's Office (ICO) how personal data processing complies with the Data Protection Act and the GDPR and the Data Protection Act 2018 when they comes into force;
- The intended outcome of a DPIA should be to identify risks to privacy and minimise these;
- Conducting a DPIA is a legal requirement under the GDPR particularly if the proposed processing is using new technologies and poses a high-risk to people's data.
- A Pre-Assessment should be carried out to identify whether or not this full assessment is required.

Further information and guidance on the DPIA is also available on the ICO website here: ICO's PIA code of practice and the Article 29 Working Party here.

GOVERNANCE ARRANGEMENTS

The DPIA may be subject to review and audit by Camden's Data Protection Officer (DPO), ICT Project Review Board, Corporate Information Governance Group (CIGG) and the Information Commissioner's Office (ICO). A decision may also be taken to publish the DPIA. You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

1. PROJECT SUMMARY

Project Name	Re procurement of Street Population Services	**Directorate and Service**	Communities/Public Health
Project Sponsor and Position	Aaron Manku, Head of Community Safety & Emergency Management	**Project Manager and Position**	[redacted] Lead commissioner rough sleeping [redacted] Commissioning Manager substance misuse
Project Start Date **Project End Date**	1st April 2019 (tender process will however commence in August after cabinet approval for the procurement strategy)	**Project Go Live Date (anticipated/planned)**	1st April 2019
Third parties involved/associated with the Project:	Focus mental health team Change Grow Live Thames Reach St Mungo's Metropolitan Police SNT Greater London Authority	**Does this DPIA cover multiple projects?**	No

High Level description of the Project: Re-procurement of Street Population Services in the borough in order to deliver a new contract by April 2019. The procurement strategy will recommend combining 2 existing contract (spectrum and SST) currently working with a similar cohort. The overall objective of the combined service will be to ensure that all those who are rough sleeping or engaged in street activity receive a service offer which means they no longer have to sleep rough or they receive a service offer which meets their health and treatment needs.

Scope of the DPIA:

Clients full needs assessment

Onward referrals to partner agencies

Recording and retaining clients data

Sharing appropriate information within a partnership setting (targeting and Tasking meetings)

Why is a DPIA required?

The project does present some risk due to the complex nature of the work, the vulnerable client group and the merging of existing work practises from two current providers. There is a strong emphasis on partnership working in designing services for the cohort and for this reason sharing sensitive information appropriately is a factor that needs consideration. The combined service proposed in the procurement strategy also represents high volume work both in terms of geographical catchment and high through-put.

2. DESCRIPTION

Description of the Project:

The re- procurement exercise seeks to combine 2 existing commissioned services as follows:

Camden Safer Streets Team – An assertive specialist outreach team designed to tackle rough sleeping in the borough. The team respond to reports of rough sleeping in the borough and provide specialist services to meet their needs. The service is delivered under the Council's Routes off the Street (RTS) strategy. The objective of RTS is to ensure that all those who come to notice for rough sleeping and related street activity in the borough receive a service offer which means they no longer have to sleep rough.

Spectrum day centre – A day centre for individuals who are homeless and street active in Camden or living in temporary accommodation in Camden and presenting with substance or health issues.

Data flow map:

Annex A. SST-Spectrum service model

Types of personal data proposed to be processed:

Personal data	What is the purpose?
Name and date of birth	To assess previous contacts with services and to determine the service options available
Housing history	To assess previous contacts with services and to determine the service options available
Substance misuse issues	To assess previous contacts with services and to determine the service options

	available
Mental health issues	To assess previous contacts with services and to determine the service options available
Criminal justice issues	To assess previous contacts with services and to determine the service options available

Types of Special Categories/ Sensitive personal data proposed to be processed:

Data concerning physical or mental health needs

Types of data subject:

Vulnerable adults with complex needs who are rough sleeping ,homeless or street active

3. SCOPE AND DESCRIPTION OF PROCESSING

Description of the processing activities:

Full assessment of client needs conducted face to face

Onward referral to specialist partner agencies

Collation of data using the Combined Homelessness Information Network (CHAIN) database

Collation of data using a data base product sourced by the successful provider

Discussion of client need/risk in a partnership Targeting and Tasking meeting

[*High level description of processing activities including technical capabilities/functionality*

Assets/technology involved with processing the personal data:

a. *Hardware- is there any equipment being used?*

   Laptops or portable devices will be used

b. *Software – what software will be used?*

   CHAIN database

   Criminal justice secure mail (CJSM) encryption software

   A client data base product will be sourced by the successful provider

c. *Networks – will the processing be on the council's network, or shared with another organisation eg the CCG?*

   Data will be securely shared across the Council's network and between networks managed by providers and partner agencies

d. *People – who will do the processing? Council staff or contracting out? What areas of workers in the organisation that is doing the processing?*

   All staff in the combined service will be processing data. Staff will be employed by the provider

e. *Paper – will you be having paper records?*

   There will be no paper records

f. *Paper Transmission Channel(s) – how will paper records be handled?*

N/A

g. *Mobile Devices (not Camden issued laptops – other devices if any)*

Outreach workers will potentially use portable devices for processing client data, sourced by the successful provider

h. *Cookies – if you are providing web services will you be using cookies? If so, what type (eg persistent)*

As per Camden IT policy or provider IT policy

i. *Other such as cloud, data warehouses etc. – will you be storing data in the cloud eg is the provider* SAAS *(software as a service)]*

Potentially office 365 will be used to share client data

Purpose and Benefits:

The purpose of processing client data will be to complete a needs assessment and progress onward referrals to housing and specialist providers as appropriate. The objectives of the combined service will be:

- Reduce the volume of rough sleeping and street activity, and the impact such activity has on the community, working in line with targets set by the GLA and central government and the Camden Routes off The Street (RTS) strategy
- Positively change the behaviour of people involved in street activity in Camden and to assist them towards sustainable independent living
- Engage with the community to address local concerns in regards to street activity
- Offer comprehensive assessment, structured, joint support planning and effective engagement with all eligible service users
- Offer clear pathways and assertive support into Camden's substance misuse treatment services

- Promote recovery and pathways into employment, education and training
- Ensure appropriate access for service users to healthcare and mental health services

Sources of the personal data: where are you obtaining the data from?

Data will be collected directly from data subjects by means of face to face assessment and street based engagement.

Feeds from systems will be obtained where appropriate including the CHAIN database.

Police data is used occasionally where there are criminal justice issues to be considered.

Length and frequency of processing:

Clients are expected to engage with the service from between 1 week to up to 3 months

Processing volumes

The combined service is expected to engage with up to 100 clients per month.

All cases will be vulnerable adults with support needs

Data minimisation:

Data minimisation, best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification.

4. BASIS OF PROCESSING

Fair, Lawful and Transparent Processing (Article 5(1)(a))

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Processing shall be lawful only if and to the extent that at least one of the requirements in Article 6(1) applies.
You must meet one of the conditions below to process the data lawfully.
Please note if you meet another condition you do not need consent. Most of the council's processing is done under numbers 1 and 4 below. There are few occasions where the council actually relies on consent.

If you are processing special categories of data then you need to satisfy one of the conditions in Article 6 **and** one of the conditions in Article 9(2)

	Lawfulness of Processing (Article 6)		
1	Is the processing necessary for compliance with a legal obligation to which the Council is subject? In other words does the council have to do this processing because there is law that says we must do so If 'yes', please identify the legal obligation and explain why the processing is necessary.	NO	
2	Is the processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract? In other words does the council have to process the data to do things it has contracted to do with the data subject?	NO	

	If 'Yes', please explain why the processing is necessary.		
3	Is the processing necessary in order to protect the vital interests of the data subject or of another natural person? It is intended to apply in 'life or death' situations, such as providing medical information to a hospital when a patient is incapable of giving consent. There won't be many times this applies for the council.	NO	(There are rare occasions where this sort of judgement would be exercised. For example where a client of no fixed abode and no settled base was receiving hospital treatment.)
4	Is the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller? In other words: are you doing council work that is in the public interest and you need to do the processing to carry out the work properly? If 'Yes', please identify the statutory powers that you are relying on and identify the task.	YES	The council processes personal date for rough sleepers in Camden and inputs data on to the CHAIN database. The data is also shared with housing providers and service providers to meet the needs of rough sleepers. Processing data on CHAIN and referral documentation will be carried out on the basis of public interest. Local, regional and central government are subject to a public duty to measure, reduce or end rough sleeping in their areas, as identified, for example, in the **Homeless Act 2002,** and the **Homelessness Reduction Act 2017.** Street Population services are commissioned by Camden Council and work with public bodies including the GLA and the metropolitan Police. These services exercise a function on behalf of the Council and its strategic partners, in order to further this public duty. Personal data is shared with the Metropolitan Police on a case by case basis to prevent crime, and reduce anti- social behaviour. This work is carried out under the auspices of the **Anti-Social Behaviour Crime and Policing Act 2014**
5	Are you relying on the individual to provide consent to the processing of their personal data for one or more specific purposes (as grounds for satisfying Article 6)? Please note if you meet another condition you do not need consent. Most of the council's processing is done under numbers 1 and 4. There are few occasions where the council actually relies on consent. If you rely on consent, the individual may withdraw consent at	NO	

	any time. You would then have to stop processing the data, unless there is another ground to rely on. An example of when consent is not needed is processing children's data for carrying out safeguarding work- this is a legal duty. An example of when consent would be the right option would be eg when carrying out sexual health testing. If YES then how and when will this consent be obtained? If NO then what alternative legitimate arrangements are in place? Is the consent in accordance with the requirements in the GDPR?		
6	Is the processing necessary for the purposes of legitimate interests pursued by the Council or by a third party? Are these interests overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child? If there are legitimate interests, please explain what these are. If the exercise of these may impact on the rights and freedoms of the data subject, please explain the potential impact. *Note that the Council can only rely on this basis in limited circumstances, when it is not carrying out one of its 'tasks'. If you think this applies to your project, you must seek advice from the Data Protection Officer at dpo@camden.gov.uk	NO	
7	Will you be collecting **Special Categories of data**, e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation? The Council also considers financial data and	YES	The service will be collecting special category data around physical and mental health

	electronic signatures to be special category data.		
8	Special Category data must only be processed if at least one of the grounds in Article 6 (outlined in numbers 1-6 above) is met and in addition, one of the requirements in Article 9(2) can be met. Which basis in Article 9(2) are you relying on to process Special Category Data?		Article 9 (2)(g) are met on the basis of substantial public interest The conditions of DPA schedule 2 part 2 "restrictions of rules" are met The requirement to also fulfil a condition from Schedule 1, Part 2 appears to be met under: Equality of opportunity or treatment,
9	If you are relying on a different basis for different categories of Special Category Data (e.g. a different basis for each type of data to be processed) then please explain here:	NO	
10	Will you be processing personal data relating to criminal convictions and offences or related security measures? If YES, Article 10 may apply. You must seek advice from the Data Protection officer at dpo@camden.gov.uk	Yes	Yes but rarely. Personal data is shared with the Metropolitan Police on a case by case basis to reduce anti- social behaviour and progress enforcement interventions as a last resort. This work is carried out under the auspices of the Anti-Social Behaviour Crime and Policing Act 2014 Legal advice is that : In relation to the Criminal Conviction data, this is would only fall under the Law enforcement Directive if it was being processed for enforcement of a particular crime. Therefore it appears that for the proposed activity, you would be collecting the data and where appropriate share with the police in accordance with the Anti-Social Behaviour Crime and Policing Act (Processing if personal data carried out under the Control of Official Authority). In circumstances where the Act would not cover the sharing of the criminal convictions data, we could look to satisfy one of the conditions in Schedule 1, namely: 1. Statutory etc and government purposes "the exercise of a function conferred on a person by an enactment or rule of

			law". This would apply where there is legislation which allows the Council to carry out the activity 2. Preventing or detecting unlawful acts, which is met if the processing: a. Is necessary for the purposes of the prevention or detection of an unlawful act; b. Must be carried our without the consent of the data subject so as not to prejudice those purposes; and c. Is necessary for the reasons of substantial public interest.
11	The council has to comply with the Human Rights Act. Article 8 is the right everyone has for respect for their private and family life, home and correspondence. The council can't interfere with this right except as the law allows and is necessary to ensure national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. You need to be sure that the processing you will do will not breach these requirements. Have you considered the requirements of Article 8 and will your actions interfere with the right to privacy under Article 8? Yes considered and NO will not interfere Have you identified the social need and aims of the project? YES Are your actions a proportionate response to the social need? YES Are you sure the processing will be in accordance with Art 8? YES		

	If you are in doubt contact the legal team for advice. In most cases if the outcome of the DPIA is that there are no high risks remaining after mitigations are in place (see below) then there should be no breaches of Art 8.		
12	Is any of the personal data being processed held under a duty of confidentiality, e.g. client confidentiality? If YES please detail	NO	
13	Is any of the proposed processing subject to any other legal or regulatory duties? If YES please list the additional legal or regulatory duties and how you will comply with these.	NO	
14	**Fair Processing and Transparency** If you have obtained information from data subjects or from a third party, there is certain information that you must provide to data subjects to comply with Articles 12, 13 and 14 of the GDPR. There are corporate policies and procedures on fair processing in place to cover these situations: https://lbcamden.sharepoint.com/sites/intranet/business-support/Pages/Data-Protection-in-Camden.aspx You must read these. Indicate here how you will comply with them.		https://lbcamden.sharepoint.com/sites/intranet/business-support/Pages/Data-Protection-in-Camden.aspx Commissioners will ensure that best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification. The contract specification will reference “data protection in Camden” pages and the “Information in Camden” documents including the 10 golden rules for data security

Purpose Limitation. Article 5(1)(b) **Personal data shall be collected for specified, explicit, legitimate purposes, and shall not be further processed in any manner that is incompatible with those purposes or those purposes.** ***Note that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.**			
15	**Uses of Personal Data within the Organisation** Will you have a procedure for maintaining an up to date record over the collection and use of personal data?	YES	
16	**Use of Existing Personal Data for New Purposes** Do you know the purposes for which the data was originally collected? **Does the project involve the use of existing personal data for new purposes?** If NO then go to question 13 If YES, how will you inform data subjects that you intend to process for new purposes (so as to comply with Articles 13 – where the data was originally collected from the data subject and 14 GDPR – where the data was originally collected from a 3rd party)	YES NO	
17	What checks have you made to ensure that processing of personal data is compatible with its original purpose?		Best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification.

<table>
<tr><td></td><td></td><td></td><td>The provider will be required to include data security as part of their standard training package for new recruits.

The new provider will put in place system checks and prompts to reference prior to sharing information.</td></tr>
<tr><td>18</td><td>Disclosures of Data
Who will you routinely share the data with?

Recipients: see annex B</td><td></td><td>Annex B provides a list of partner agencies the service will be working with in order to progress referrals and make service offers which meet their needs.

Data shared include the information below:
<table><tr><td>Name and date of birth</td></tr><tr><td>Housing history</td></tr><tr><td>Substance misuse issues</td></tr><tr><td>Mental health issues</td></tr><tr><td>Criminal justice issues</td></tr></table>
All of the providers listed are subject to data sharing arrangements with street based services commissioned by the Council.

Prospective providers will be asked to ensure that they have data sharing arrangements in place during the implementation phase of contract delivery.</td></tr>
<tr><td>19</td><td>How will your team be made aware of the requirements for sharing with third parties?</td><td></td><td>Best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification.

It is anticipated that providers will identify system checks and prompts to reference prior to sharing information.</td></tr>
</table>

20	How will you make data subjects aware of their rights?		A privacy notice/data protection statement will be made available on first contact to new clients as per the GDPR compliance aspect of the contract specification.
'Data Minimisation' Article 5(1)(c) : **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**			
21	**Adequacy and relevance of Personal Data** What arrangements/procedures/ measures are in place to determine the adequacy and relevance of the personal data being collected and processed for each purpose, and to ensure that it is not excessive (e.g. ensuring that only minimum required amount of data is collected and processed)?		Data minimisation, Best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification.
22	What arrangements/ procedures/ measures are in place to ensure that data collection and processing procedures are and will remain adequate, relevant and not excessive in relation to the purpose for which data is being processed?		Best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification. The provider will be expected to review procedures regularly to ensure compliance is sustained.
Accurate and up to date Article 5(1)(d): **Personal data shall be accurate and, where necessary, kept up to date.**			
23	Have you assessed the risk to the individual and the Council with respect to the consequences that could be caused through; 1) Inaccuracy of data and; 2) Holding data that is out of	YES	

	date? If NO then please explain.		
24	What arrangements are in place to check the accuracy of the data with the individual?		Client details will be checked for accuracy with the client themselves and referenced against the CHAIN database where information is unclear or needs to be verified
25	Will accuracy checks cover free text fields including comments about individuals?	YES	All data used to offer services to individuals and progress onward referrals will be checked for accuracy
26	How will you determine when and how often personal data would require updating?		When new referrals are made data will be updated. There is not a fixed timeline for this as it would depend on individual circumstances, however if a client has disengaged from services the expectation is that the provider would always re-assess the client for example.
27	What arrangements are in place to for individuals to notify you if they believe their data to be inaccurate?		A privacy notice/data protection statement will be made available on first contact to new clients as per the GDPR compliance aspect of the contract specification. The document will include a means of contact the data owner if the data subject believes their data to be inaccurate.
28	How will you ensure that inaccurate or out of date data is erased or rectified without delay?		Best practise in data security and GDPR compliance will be required to be demonstrated under the tender process and included in the service specification. The provider will be expected to present a procedure setting out ways that inaccurate data will be erased.

Storage Limitation Article 5(1)(e):

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject

29	Is the data in question intended to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes? If YES, how will you satisfy the requirement in Article 89(1)?	NO	
30	**Retention Policy** Is there a corporate data retention policy that covers the data processed under this project? If YES then go to question 27. If NO then seek advice from the Information and Records Management Team	YES	
31	How will you determine when the data is no longer necessary for the purposes for which it was collected? Who will be responsible for reviewing the data?		The necessity for the data will be determined by individual circumstances and the progress of outcomes. The corporate retention policy will also determine the length of time that data is retained and provide a framework for decision making. The provider will be responsible for reviewing the data
32	If the data is held on an IT system then will this system flag records that due for review/deletion? If NO then please explain	YES	
33	Will there be any exceptional circumstances for retaining certain data for longer than the normal period? If YES then please explain.	YES	The necessity for the data will be determined by individual circumstances and the progress of outcomes. The corporate retention policy will also determine the length of time that data is retained and provide a framework for decision making.
34	**Destruction of personal data** Are there arrangements over the secure deletion/destruction of personal data? If NO then please explain.	YES	

'Integrity and Confidentiality'. Article 5(1)(f): **Personal Data should only be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**			
35	When answering the questions below, you need to consider what technology is available and how much this would cost to put in place. You need to balance that against the type and amount of processing and the nature and severity of risks to the data subjects to ensure that the GDPR will be complied with (particular reference to Article 24). For example, where there is extensive processing and higher risk, it would be appropriate to implement a much more costly solution than if the processing was minimal or negligible risk.		
36	**Security Measures** Outline the technical or organisational measures that covers the protection of personal data and processing activities under your project		All meetings are paper free and client information is provided on a screen All data is transmitted on-line using encryption software (CJSM) The new provider will be responsible for upholding this practise and developing procedures during the implementation phase of contract delivery
37	Who will be responsible for enforcing compliance with the council's corporate security policy?		The Lead commissioner for rough sleeping and commissioning manager for substance misuse will be responsible for ensuring compliance with the council's corporate security policy
38	**Contingency planning - Accidental loss, destruction, damage to personal data** Have you assessed the risks and put in place mitigating controls to minimise the risk of data loss through: • Human error or theft;	YES	

	• Computer virus or network failure; • Fire, flood or any other disaster? If NO then please explain.		
39	Do you have procedures to recover data (both automated and manual) in the event that data is lost? If NO then please explain. **Practical safeguards:** *[How will you control who has access to the data?* *What training, communications and awareness will be carried out to make sure the data will be processed lawfully?* *Will you carry out due diligence to make sure that third parties involved* *adequate and subject to a legal obligation (e,g, a contract) to make sure they process the data lawfully?* *What contract management and monitoring arrangements will be put in place with third parties?]* **Mechanisms to protect personal data:** *[Examples: De-identification of data* *Examples: Arrangements re destruction of data* *Examples: Data back up/disaster recovery arrangements]* **Mechanisms to demonstrate compliance with legislation:** *[Examples: Maintenance of records such as re: consents, privacy*	YES	

	Are there separate measures to protect special category personal data? If NO then please state why the measures above are sufficient. **There is a corporate procedure for detecting and reporting breaches of security (remote, physical or logical) and this must be followed in the project. Any third parties or sub-contractors involved in processing the data must be made aware of this procedure and measures taken to ensure they comply with this.** Confirm this is the case and outline how it will be achieved**.**		

5. TRANSFERS OF DATA OUTSIDE OF THE EEA -will any personal data be processed outside of the EEA? This includes information processed on servers based outside the EEA as well as processing carried out by sub contractors. This is unlikely to apply to the Council but you must take advice from the Data Protection Officer if this is relevant to your project. N/A

Country to be transferred to: *[Provide a list of all the countries that the personal data will be processed in]*
Hosting location: *[Identify where the data will be held. You may require IT advice in this regard as you may need to consider data being held on the cloud]*

International data transfer arrangements: *[describe how the data will be transferred outside of the EEA]*
Name and role of parties receiving the personal data:
Legal safeguards for the transfer: you need to seek DPO advice before completing this *[EU Model Clauses* *Privacy Shield]*

6. ARRANGEMENTS TO ADDRESS INDIVIDUAL DATA SUBJECT RIGHTS - THESE MUST BE DEALT WITH IN ACCORDANCE WITH CORPORATE POLICY which is set out in Information in Camden on essentials~~d~~]. They include the following and you must be aware of these rights.
If they are of specific significance to your project then you must state how you will deal with these, otherwise it is assumed they will be dealt with in accordance with the council's standard policy.

Right to be informed: they will be dealt with in accordance with the council's standard policy.
Right of access: they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed

Right to rectification:

they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed

Right to erasure/right to be forgotten: they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed
Right to object and restrict processing: they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed
Right to data portability: unlikely to apply but they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed
Rights in relation to international transfer(s): not applicable but they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed
Rights in relation to prior consultation: as detailed in 7
Rights in relation to automated decision-making and profiling: unlikely to apply but they will be dealt with in accordance with the council's standard policy, although we will deal flexibly with the ID required given the circumstances and will take advice from the IRM team as needed

7. CONSULTATION WITH INTERESTED PARTIES

Input of data subjects and/or their representatives and other stakeholders (for example a residents' association or business):

[Is your project going to effect a change which will have a direct impact on data subjects, for example: introducing CCTV into a library? If so, you need to consult with data subjects, their representatives and other stakeholders.]

Input of data subjects will be obtained by consulting with "voicability", service user forum. In addition a service user will be invited to participate in the tender panel for re-procurement process.

- Final decision - if different from Data subjects' views to include rationale for proceeding

- Justification for not seeking input from Data subjects for example, compromises confidentiality of business plans, disproportionate, impractical.]

Input of experts and other interested stakeholders:

[Record the advice/input of independent experts of different professions (such as lawyers, IT experts, security experts,) as well as other stakeholders who have an interest in the Project, such as a business affected by the project.]

Camden Homeless Health Network will be invited to view and comment on the draft specification.

8. PRIVACY RISKS

This section should be used to identify the risks and specify measures and safeguards that will be implemented to ensure that personal data is protected and processed in compliance with the GDPR and Data Protection Act. This section is also a method of recording the risks and monitoring their implementation of mitigating measures. Add rows to this table as necessary.

RISK	MITIGATION	OWNER of ACTION	TIMESCALE	RESIDUAL RISK

Identify and Describe the Risk	What is the Mitigating measure?	Who is responsible for ensuring mitigating measures are implemented and how?	Timescale for Implementation?	Once the mitigating measures are put into place, what is your assessment of the level of residual risk?
1. Personal data forwarded to partner agencies by e-mail could be accessed by unauthorised people.	The provider will be required to use encryption software, CJSM or as prescribed by the Council.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option April 2022-March 2024	low
2. Accidental loss of personal data recorded or transported on paper documents	The provider will be required to demonstrate a paper free operating system. All multi agency meetings will be paper free for example.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery. Data security breaches will reported to the Council within 72	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022	low

		hours and near misses will be reported to the commissioner for learning and reflection.	Extension option April 2022-March 2024	
3. Data is shared with third parties in ways which is not compatible with the original purpose	The provider will be required to include data security as part of their standard training package for new recruits. The new provider will put in place system checks and prompts to reference prior to sharing information.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option April 2022-March 2024	low
4. There is insufficient transparency and clarity of purpose as to why personal data is being collated by the provider and for what purpose.	A plain English privacy statement based on the Camden public privacy statement will be issues to all clients by the provider at first contact statementhttp://www.camden.gov.uk/privacystatement	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option	low

			April 2022-March 2024	
5. Client data processed by the provider is inaccurate	Client data will be verified by full assessment with each client away from the chaotic street setting. Where appropriate details will be verified using the CHAIN database.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option April 2022-March 2024	low
6. Client data is held for longer periods than is appropriate	Client data will be retained in line with corporate policy however the likelihood of recidivism or return to the streets makes it possible that that up to 7 years is required for complex cases. This will be determined on a case by case basis, as clients needs and risks are different for each individual.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option April 2022-March 2024	low

7. Systematic and high volume processing takes place for clients including those in a street based setting	All data will be inputted to secure Hand held device and no portable paper records will be obtained. The provider will be required to include data security as part of their standard training package for new recruits. Wherever possible face to face assessment will take place away from the street setting at the Spectrum day centre.	The provider (project manager) will be responsible for implementing the measure. Commissioners will be responsible for checking during the contract lead in period and during contract delivery.	Lead in period –Q4 2018/2019 Contract delivery April 2019 – March 2022 Extension option April 2022-March 2024	low

Overall risk rating before mitigation: Low Medium **High**

Overall risk rating after mitigation : **Low** Medium High

If the risk of the intended processing still remains high, despite mitigating measures being put in place, there may be a duty to consult the ICO before any processing takes place (Article 36). You must take advice from the Data Protection Officer.

9. DPO Advice and Consultation

Officers must seek the views of the DPO when carrying out a DPIA. Use this section to record the advice, attach additional documentation in appendix B if required**:**

ADVICE OF DPO

Advice of DPO:

Date of the advice:
Does the DPO advise that ICO consultation is required? If so, record here how that will be actioned: **See 11 below.**

10. DECISION

Decision: *[Proceed with Initiative/Not proceed with Initiative/ Other]*
Authorised person:

11 CONSULTATION WITH ICO

If the DPO advises that consultation with the ICO is required this will be undertaken by the DPO (or by Business Support staff who deal with data protection under the instructions of the DPO). There will be consultations with services and

project sponsors as needed.

Date ICO consulted:

Attach documents sent to ICO in Annex C.

Date ICO reply:
ICO Case Officer:
ICO reference:
ICO decision in summary:
and attach formal notification in Annex D:

OUTCOME

Based on ICO ruling detail the outcome for the project:
What steps need to be taken:
Update the PIA risks is section 8 and reassess the risk based on ICO advice.

DPO Comments:

ANNEX A
DATA FLOW MAPS

ANNEX B
DPO ADVICE - add in anything not included in 14 above

ANNEX C – Documentation sent to ICO

ANNEX D – ICO Response

DOCUMENT MANAGEMENT

Document history:

Version number	Summary of change	Date	Reviewed by