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	Outsourcing addressing waiting lists for assessments and reviews in Adult Social Care's Support and Safeguarding Service	
Project Lead and Information Asset Owner/s	Project Lead	Avril Mayhew, Head of ASC Operations
	IAO name and asset	Avril Mayhew, Head of ASC Operations
	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 Support and Safeguarding Service (S&S) in Adult Social Care (ASC) is responsible for undertaking statutory assessment and reviews of care and support under the Care Act 2014. These involve assessing the needs of vulnerable adults and identifying what support is to be provided to best meet those needs.	

	The Service is experiencing capacity challenges with its existing workforce being able to address the backlog of assessments and reviews and allocate work. The Service is also experiencing recruitment challenges in being able to externally recruit both permanent and/or locum staff with the appropriate skills and experience required to tackle the backlog of waiting lists. This is impacting on the service we deliver to residents, as well as staff morale. The Service has therefore identified a requirement to engage an organisation to provide additional capacity to undertake initial assessments and reviews in order to reduce its waiting lists and/or to undertake reviews as part of our MTFS savings targets. It is likely that c500 such actions will be within scope. The organisation procured will require access to Mosaic. Whilst the initial assessments and reviews are currently undertaken, the provision of a 3rd party to undertake them with the concomitant processing and access to systems is new processing.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	September 2023

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.



DPIA%20Pre-Screen
%202023%20updatec

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?**						New/Changed			
							Changed			
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate									
	<u>Personal Data</u>									
	Name	**<u>Y</u>**	Date of Birth	**<u>Y</u>**	Gender	**<u>Y</u>**	National Insurance Number	**<u>N</u>**	Financial Information about the person	**<u>Y</u>**
	Address	Y	Email address	Y	Telephone number	Y	NHS No	N	Other eg a reference number such as Mosaic ref	Y
	Other data *(Please state):*		See notes in the other data special categories of personal data for full list of information which can be viewed.							
	<u>Special Categories of Personal Data</u>									
	Racial or ethnic origin	Y	Fingerprints/ Biometrics	N	Religious or philosophical beliefs Political opinion					Y

	Trade Union membership	N	Physical or mental health or condition					Y
	Sexual life or sexual orientation	Y	Housing records Social services records	Y	Tax, benefit or pension records	N	Employee/HR records	N
	Other data *(Please state):*	The following data which is stored on Mosaic can be viewed: • Name • Addresses • Telephone number • Email address • Ethnicity • Gender • Marital Status • First language • Fluency in English • Nationality • Personal relationships (with others listed in Mosaic) • Country of Birth • Date of birth • GP details • Health information • Disabilities					

		• Sensory needs information (determined by service user group_ • Financial information (relating to whether someone has a care package or is under PFS) • Relevant criminal convictions • Warning and general notes • Sexual orientation • Case notes • Support plans • Other workflows may be read which have been noted in previous sections. Religion can also be listed under basic details, although this isn't something usually recorded. Workers may not be able to see the detail of some of the information listed above, however, the front screen of a person's profile on Mosaic is likely to provide at least an indication of each category. Mosaic contains records from Children Services. The organisation procured are only providing provide a service for Adult Social Care. Children's (CSSW) records should not be accessed.
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Mosaic does include information on relevant criminal convictions.

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!**	The Support and Safeguarding Service within Adult Social Care has identified a requirement to engage an organisation to provide additional capacity to undertake initial assessments and reviews in order to reduce its waiting lists and/or to undertake reviews as part of our MTFS savings targets. This is in line with the Care Act 2014. The organisation procured will require access to Mosaic. This is to check for eligibility and also to give a full picture of the case when undertaking assessments and reviews on behalf of Camden Adult Social Care. They can also use this information to highlight any relevant information to Adult Social Care such as safeguarding matters, payment matters with the Direct Payment Team or assessments which Adult Social Care need to undertake. Records of the assessments and reviews that will be carried out by the organisation procured will be recorded on Mosaic. The organisation procured will be able to make amendments to Mosaic, for example add information on new people, update existing contact information for people on Mosaic, and they can add case notes to Mosaic. The organization procured will be able to read and workflows including: three conversation workflow (including Reviews, OT, Sensory and Outreach work). All other workflow on Mosaic is either visible but the contents

		cannot be read, or no access has been granted at all (depending on the type of work). Workflows and access are subject to change, this is a managed process led by the Adult Social Care Senior Business Analyst and in relation to access the Prevention and Wellbeing Service Manager. Camden Council are committed to sharing with people the record of their assessment. If data is extracted from Mosaic for this purpose all checks are made to ensure this is done securely. The procured organisation is unable to save data outside of the Camden network. There may be correspondence between ASC and the procured organisation, usually by email, if there are questions about a case or if a budget needs to be approved or a referral made. The minimum of personal details are shared and the procured organization will only use initials and Mosaic numbers in their correspondence if necessary.
3.2	**Explain in as much detail as possible why this is being done**	The Service is experiencing capacity challenges with its existing workforce being able to address the backlog of assessments and reviews and allocate work. The Service is also experiencing recruitment challenges in being able to externally recruit both permanent and/or locum

		staff with the appropriate skills and experience required to tackle the backlog of waiting lists. This is impacting on the service we deliver to residents, as well as staff morale. For the week commencing 22nd May 2023, there were a total of 1,017 immediate pieces of work awaiting follow up and/or allocation across the S&S Service; 762 in the Access and Response team, and 255 across all of the neighbourhood teams. There was also a total of 966 outstanding annual reviews (i.e. statutory annual reviews that have missed the 12-month timeframe). The Service has therefore identified a requirement to engage an organisation to provide additional capacity to undertake initial assessments and reviews in line with current needs.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**	Yes. All audit checks on Mosaic including Disclosure Barring Service checks, signed Acceptable Use Policy and training are followed before access is granted.

	External organisation or partner Name	**Controller or Processor?**	**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**
	TBC – going through procurement process	Processor	In progress
3.4.	**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.**		See the DPIA. DPAT agree no flow chart needed.
3.5	**How will you handle data in your project, how will use store and share it. Please explain**		The procured organisation will access Mosaic. Occasionally and upon request pseudonymised data (by Mosaic reference number) is extracted from Mosaic and will be sent by secure email. The organisation will have passed due diligence checks to ensure it has a solid track record and will meet necessary standards. Their staff who get access will be suitably qualified and experienced and have been vetted on appointment and have clean enhanced DBS checks.

		The council will monitor their access to ensure its relevant and appropriate to the task given to them

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)(e) processing is necessary for the performance of a task carried out in the public interest.	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** GDPR Article 9 (2) – Special Category Personal Data Processing a) social protection law - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition**

		security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject. b) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. *the DPA18 Schedule 1 Part 1 condition met is para 2 health and social care purposes* h) provision of health or social care - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the	

		provision of health or social care or treatment or the management of health or social care systems and services Use of this article requires that the Data Protection Act Section 10(2) be satisfied. *the DPA18Schedule 1 Part 1 condition met is para 2 health and social care purposes* *for both 9(b) and (h) the underlying law is the Care Act 2014.*	
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**		
	Consent is not the lawful basis for this work.		
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		
	We may want to consider creating a specific worker role to limit the organisation's access to workflow within Mosaic adults. All staff would undertake appropriate Mosaic training, have a DBS with both adult		

	and children list checks and have signed an acceptable use policy. Audit checks will be in place to check for errors in information recorded and gaps in information.	
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 - The adults privacy notice will be amended to explain what is being done and who the contractor is
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?**	
	We will comply with any Subject Access Requests and other data subject rights. All data is stored within Mosaic. Any SARs etc will be responded to under the council's existing processes	
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?**	
	Personal data will stop being used after there is no legal reason to use it. To note, that data held in Mosaic is not currently removed after it is no longer required. This is an identified risk held by ASC SMT and is something that will be addressed, so data retention in line with our corporate retention schedule.	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, SharePoint, shared drives,*
	Mosaic
5.2	**In what country is the data stored?**
	Mosaic data is stored on Camden servers that is controlled in London. When Mosaic moved to the cloud (in around October 2023), the data will still be stored in the UK, in a cloud data storage solution.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	A limited number of staff from the procured organisation would have access.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Access is agreed with Adult Social Care (either Executive Director of Adults and Health; Head of ASC Operations; Head of Neighbourhoods; Head of Support and Safeguarding Transformation; or, Prevention & Wellbeing Service Manager). All staff would undertake appropriate Mosaic training, have a DBS with both adult and children list checks and have signed an acceptable use policy. The procured organisation's staff will be set up on Camden's network, and added to Active Directory with a specific 'external account' so that they will be able to log in to Mosaic. The procured organisation will provide corporate encrypted devices and will be provided with access to Global Protect to enable them to access Camden's network and then login to Mosaic with their accounts set up.

5.5	**Is there an ability to audit access to the information?**
	Yes. A specific worker role can be created to limit access to workflow within Mosaic adults. Audits of the records the procured organisation look at can also be undertaken by the Mosaic Super User and Digital Skills Trainer to ensure that only appropriate records are accessed. Samples can be taken approximately every month as part of this audit process.
5.6	**What security and audit measures will there be to make sure that data is kept safe?**
	Mosaic holds the most sensitive resident data. Whilst the organisation will have limited access, they will still be able to view sensitive data. We will ensure that expectations of handling this sensitive data are understood, by providing training, regular auditing of records the organisation have accessed, ensuring an acceptable use policy is signed and that staff with access to Mosaic have a DBS check, with both barred checks. Global Protect will be set up on corporate encrypted devices so they can securely access the Camden network and Mosaic.
5.7	**Has the Information Security Team advised on the security measures? What were their comments?**
	Staff would require an Advanced DBS, restricted access roles on their mosaic accounts with specific access on a need to know basis. Monitoring or Logging of data being accessed.

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**
Privacy Intrusion – sensitive data being shared internally or externally with people that did not need this information (did not need to know) or unintended third parties (should not know). Compliance risk: unrestricted control of the data to parties beyond the scope of this assessment and understanding of what is/is not legally processable. Corporate risk: breach of GDPR legal processing, legal risk and loss of trust of data subjects. Increased risk to data subject if information shared with third party.	Possible	Moderate	9

Misuse of data: Data could be used in a manner incompatible with the data sharing agreement. Data is shared with other teams or third parties other that it is being legally processed. Examples include: access to adult records that aren't for the purposes of undertaking assessments/reviews for the individual. This comes with a compliance risk as individuals/teams/services may have access to information on the data subject and could use this for other reasons than completing assessments and reviews. This may have legal implications, and a corporate risk, breach of GDPR legal processing, risk from any appeals or legal challenges as data is being used in a way that wasn't intended. This may also come with a reputational risk for the Council.	Likely	Moderate	12
Access violation: Access to Mosaic is inappropriately given to staff or not taken away after a person leaves the organisation. If people are not adequately trained on Mosaic they may make mistakes in using the system that lead to potential data errors in recording (poor data quality) or in the worst case getting inappropriate services. If DBS checks are not taken then there are risks that people would gain access to Mosaic inappropriately, for example a DBS would flag criminal convictions that you may consider inappropriate for Mosaic access.	Possible	Moderate	9

This comes with a compliance risk as individuals/teams may have access to information on the data subject and could use this for other reasons than completing assessments and reviews. This may have legal implications, and a corporate risk, breach of GDPR legal processing, risk from any appeals or legal challenges as data is accessed by people inappropriately. It could lead to data breaches. This could potentially lead to service delivery and reputational consequences if records are inappropriately accessed, and data quality is poor. This may also come with a reputational risk for the Council.			
Data sharing with third parties (not the procured organisation) – data shared with third parties which is not controlled in line with this assessment. Third parties not storing or controlling the data in a secure and responsible way. Risks around access to this data. Compliance risk: data is access by unauthorised parties. Data is stored in such a way that it is easily accessible to people not permitted to access it. Corporate risk: As the data controller we have responsibility to ensure that all data is processed correctly by partners. Risk to data subject if information shared inappropriately. With associated reputational risk.	Possible	Major	12
Data Breach: Staff from the procured organisation may take data from Mosaic and use it for criminal activity or access of records of people	Rare	Catastrophic	5

known to them. Processing would occur that the person would not consent to. Data is lost or sent to unauthorised parties, including internal staff who are not meant to see the data. Compliance risk: ASC officers or the procured organisation making mistakes or not taking correct steps to minimise the risk. A corporate risk if the data subject challenges the organisation around the data breach. This would have reputational and financial consequences, especially if reporting is required to the ICO. This would also add to stress and open them up to possible scams etc.			
Data collection – data not collected and processed in line with this assessment. Not fully understanding or using the incorrect GDPR basis for the processing of these data. Compliance risk: data subjects are not informed or misinformed about the reasons for collecting this data. Corporate risk: data subjects challenge the council if they do not feel that their data is processes correctly. Scrutiny from ICO.	Unlikely	Major	8
Poor Data Quality: If data is not recorded correctly in Mosaic then this could have an impact on service delivery and reputational risk, with people not receiving appropriate and timely services. This could also increase the person and their family's stress and also lead to inappropriate statutory reporting. Poor data quality also a DP risk as a result of data inaccuracy and processing implications.	Almost certain	Medium	15

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?**
Privacy Intrusion	Regular audits and reviews of access to Mosaic are undertaken. Quality assurance checks and audit processes are in place and take place regularly. Consistent process to gain access to Mosaic is followed for everyone, including DBS, AUP and appropriate training. Data is not taken outside of Mosaic unless it is pseudonymised. Staff are trained in data use and so if a copy of the conversation or review is given to the person necessary checks are made.	Reduced (unlikely and moderate)	6	Moderate - yes

Misuse of data	Regular audits and reviews of access to Mosaic are undertaken. Explore separate worker role in Mosaic for the procured organisation. There are audits of this worker role to check which cases are being accessed. Contract monitoring with the organisation will take place regularly. Quality assurance meetings.	Reduced (unlikely and moderate)	6	Moderate - yes
Access violation	Consistent process to gain access to Mosaic is followed for everyone. Periodic access reviews are undertaken. If people are identified their access is removed and appropriate reporting takes place. Training is given on how to use Mosaic and ad hoc refresher training given.	Reduced (rare and moderate)	3	Low - yes
Data Sharing with Third Parties (not the procured organisation)	Quality assurance checks and audit processes are in place and take place regularly. Data is not taken outside of Mosaic unless it is pseudonymised. Training is given on how to use Mosaic and ad hoc refresher training given.	Reduced (unlikely and moderate)	6	Moderate - yes

	Staff are trained in data use and so if a copy of the conversation or review is given to the person necessary checks are made.			
Data Breach	Regular audits and reviews of access to Mosaic undertaken. Contract monitoring with the organisation will take place. Quality assurance meetings. Training is given on how to use Mosaic and ad hoc refresher training given. Staff are trained in data use and so if a copy of the conversation or review is given to the person necessary checks are made.	Same (rare and catastrophic)	5	Moderate - yes
Data Collection	Quality assurance checks and audit processes will be in place and take place regularly. Training will be given on how to use Mosaic and ad hoc refresher training given. Staff are trained in data use and so if a copy of the conversation or review is given to the person necessary checks are made.	Reduced (rare and moderate)	3	Low - yes

	Contract monitoring with organisation will take place regularly.			
Poor Data Quality	Quality assurance checks and audit processes will be in place and take place regularly. Training will be given on how to use Mosaic and ad hoc refresher training given. All conversations and reviews are signed off by ASC (Digital Skills Trainer, Prevention and Wellbeing Service Manager or Head of Transformation and Performance).	Reduced (possible and minor)	6	Moderate - yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Medium: Although appropriate contract monitoring and auditing measures are in place, Mosaic holds the most sensitive resident data, and as such there will always be an element of risk in providing access to this data, the impact of which could be significant if the risk is not appropriately managed and permissions are violated.				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	No, Sarah Laws, Data Protection Manager
DPO advice	Cleared, Andrew Maughan DPO August 2023

Information Asset Owner acceptance of residual risks	Names of IAOs
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted]

Version Control

Version	Reason	Date	Author(s)
1.0	**New draft**	**August 2023**	[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

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

Table 4: is the risk level acceptable?

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?)* • b) *What would be the harm in not processing this data?* •
2. *Data Bias* a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?* • 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?

•

*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**)*

•

*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)*

•

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

•