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	Integrated Front Door (IFD)	
Project Lead and Information Asset Owner/s	Project Lead	Camden LA: [redacted] Tavistock and Portman NHS Trust: [redacted]
	IAO name and asset	Rashida Baig, Director of Children's Safeguarding and Social Work
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 aims of the Integrated Front Door (IFD) Project are to create a central point of access for early help, social care and mental health referrals in order to improve referral pathways, reduce delays in access to services, and ensure families are directed to the most appropriate service for their needs. Dealing with mental health and social care issues separately can be more time-consuming and costly than appropriately considering and addressing needs with all the relevant professionals at the outset. Introducing an Integrated Front Door provides the function of pulling different services together to support CYP when needs are complex, from the beginning. In May 2021, Supporting People DMT committed to bringing together referrals for children's mental health and social care under a central point of access. The aim is to enable children's needs to be assessed holistically, give them the right help at the outset, and reduce delays in getting the right service(s). This idea has already been introduced and is working well in other boroughs, including LB Islington since 2019.	

	Doing the above would involve merging aspects of the Children's Contact Service (LB Camden) and CAMHS Intake (Tavistock and Portman NHS Foundation Trust) to create an Integrated Front Door (IFD). All referrals coming through LB Camden's Contact Service from GPs etc would be assessed by LBC professionals for safeguarding concerns, and then directed to the relevant service. Where a joint approach between social work and CAMHS may be required, an 'IFD daily discussion' would be held with a T&P CAMHS clinician, LBC social worker and LBC early help practitioner. They would discuss and agree the best approach and what service(s) would be most appropriate. Referrals will be made to LBC early help or social work etc and/or T&P CAMHS as appropriate. A privacy notice will be produced and shared via the London Borough of Camden website (and the Tavistock and Portman NHS Trust website). Only council employed staff will have access to the Mosaic system where referrals are loaded. Case discussions will take place between multi-agency professionals. If there are referrals where there is also a mental health concern these would be shared with CAMHS and uploaded to Carenotes.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	1 February 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.

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?	Yes
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?	Yes
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?	No
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?**	New/Changed							
		Personal data is already used to offer children, young people and families support. The change here is that CAMHS referrals (containing personal data) will be shared with the Council, as well as the NHS Trust, which would usually receive those referrals directly. CAMHS referrals are made with the consent of young people and/or their parents/carers as these are for medical intervention/assessment/treatment.							
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	**No**	Financial Information about the person	**No**
	Address	Yes	Email address	No	Telephone number	Yes	NHS No	Yes	Other eg a reference number such as Mosaic ref	Yes
	Other data *(Please state):*	Contact details of the parent/carer							
	Special Categories of Personal Data								
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics	No	Religious or philosophical beliefs Political opinion					Yes
	Trade Union membership	No	Physical or mental health or condition							Yes
	Sexual life or sexual orientation	No	Housing records Social services records	No	Tax, benefit or pension records	No	Employee/HR records			No
	Other data *(Please state):*									
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Yes								

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!**	Children and young people's mental health services (CAMHS) referrals will be brought together with early help and social care under an integrated front door. The existing Common Assessment Framework which is currently used for early help and social care referrals has been tweaked with additional relevant questions. This is to seek information about children's mental health concerns, presenting issues and what service the referrer is requesting. There is also a question asking referrers to explicitly state they have gained consent from the young person/or parent/ carer depending on the young person's age when making a referral for CAMHS. It is noted that referrals for social work child safeguarding do not need consent and the form covers these different situations. The aspect of the Integrated Front Door, which is new, concerns referrals for CAMHS services. When they are received by MASH in the IFD, all contacts and referrals will be uploaded to Mosaic. All referrals will be screened for safeguarding concerns and an appropriately qualified professional from the London Borough of Camden will decide whether there are no safeguarding concerns – if there are no safeguarding concerns and the referral is for CAMHS, then the referral would be passed on to the CAMHS Intake Team (Tavistock and Portman) and closed to MASH. The CAMHS Intake Team would input the data onto NHS Carenotes, as they usually would, and progress with the case from there. If there are safeguarding concerns, the MASH team would send the referral to CSSW. If there are no safeguarding concerns but Early Help support is deemed appropriate, the referral will be sent to Early Help to make a decision on trajectory. These referrals may be open to both the Council and CAMHS as they may require a joint approach. Joint approaches would be discussed at IFD daily discussions, which will be led by appropriately qualified professionals across both social work/ early help and children's mental health.
3.2	**Explain in as much detail as possible why this is being done**	The aims of the Integrated Front Door (IFD) Project are to create a central point of access for early help, social care and mental health referrals in order to improve referral pathways, reduce delays in access to services, and ensure families are directed to the most appropriate service for their needs.

<table>
<tr><td></td><td></td><td colspan="3">Similar projects have been implemented in other parts of the country, including in the London Borough of Islington, since 2019. LBI's central point of access was highlighted by Ofsted as an example of good practice in a recent inspection.

Dealing with mental health and social care issues separately can be more time-consuming and costly than appropriately considering and addressing needs with all the relevant professionals at the outset. Introducing an Integrated Front Door provides the function of pulling different services together to support CYP when needs are complex, from the beginning.

Finally, referrers such as schools and GPs who make referrals to MASH and CAMHS are not always aware of the range of services in Camden and could benefit from their referrals being centrally screened to enable them access to a range of services they may not have automatically considered on their own.</td></tr>
<tr><td rowspan="3">3.3</td><td>Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td colspan="3">Yes, the Tavistock and Portman NHS Foundation Trust would usually receive CAMHS referrals directly, but these referrals will now be passed onto them from the MASH in Camden.</td></tr>
<tr><td>External organisation or partner Name</td><td>Controller or Processor?</td><td colspan="2">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>Tavistock and Portman NHS Foundation Trust</td><td>Processor and then potentially controller (as cases are passed onto CAMHS and close to MASH).</td><td colspan="2">There will be a data sharing agreement between the Council and the T&P Trust for the provision of CAMHS however another DSA may need to be produced for this project.</td></tr>
<tr><td>3.4.</td><td>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 colspan="3">See appended flow chart.</td></tr>
<tr><td>3.5</td><td>How will you handle data in your project, how will use store and share it. Please explain</td><td colspan="3">Data will be stored on the Council's IT System; Mosaic.</td></tr>
</table>

		Transferred to CAMHS colleagues via bespoke Mosaic workflow in PDF format to be uploaded to the NHS CareNotes system. Data will be shared via analytical data reports that will be drawn down quarterly.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify the Lawful Basis for processing personal data/special category /criminal data.** **The lawful basis is for the IFD processing by LBC rather than the existing work undertaken by LBC and T&P.**		
	Personal data Article 6(1) UK GDPR condition 6(1)(e) public task and 6(1)(c) legal duty	**Special Category data UK GDPR Art 9 condition 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 (e) the provision of social care and (f) the management of health care systems or services or social care systems or services, with the underlying laws for both 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** The art 6 condition is the same as for personal data and the DPA18 schedule conditions are the same as 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**		
	Consent is not the lawful basis for processing the data. In some cases eg referrals for CAMHS GPs etc will need consent from the person for the *referral* but the *data processing* legal basis will not be consent.		
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		
	All data is collected solely for the purpose of processing requests for services within the IFD, including mental health, social care and early help services, and will not be passed on to other services except to secure further support from agencies or as necessary or permitted by law, for example under existing data sharing agreements. Referrals will be made via an updated Common Assessment Framework referral form which the London Borough of Camden has been using for many years.		
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. This is covered in the Council and Trust's privacy notices.	
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, we would comply with the council's policies on Subject Access Requests and other data subject rights. The other party is a data controller and the DC responsibilities will be contained in the DSA		
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?**		
	Data kept on Children in Need on Mosaic for 25 years.		

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, SharePoint, shared drives,*
	Mosaic CareNotes – for referrals that are for CAMHS
5.2	**In what country is the data stored?**
	England
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	MASH/ Early Help Services at the London Borough of Camden CAMHS Intake Team at the Tavistock and Portman NHS Foundation Trust
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	MASH Screening Officers have role-based access to part of the Mosaic System.
5.5	**Is there an ability to audit access to the information?**
	Yes.
5.6	**What security and audit measures will there be to make sure that data is kept safe?**
	Mosaic is a secure and confidential system that is only accessed by staff who have DBS clearance and access the system as part of their roles.
5.7	**Has the Information Security Team advised on the security measures? What were their comments?**
	Not required

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 by one or both of the parties in a manner incompatible with the project. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.	Likely	Major	High
Privacy intrusion: the sharing of referrals intended for only CAMHS with the council means different and additional professionals will see the sensitive information which is privacy intrusive. Whilst GPs and other referrers should inform people this may not always be the case	Likely	Moderate	Medium/high
Unexpected sharing: the council receiving CAMHS referrals and therefore holding and potentially sharing information which data subjects would not expect and privacy intrusion connected to that.	Likely	Moderate	Medium/high
Data breaches through insecure sharing, cyber-attack or similar.	Likely	Catastrophic	High Risk

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	Staff with access to data are appropriately trained in data protection requirements and there are existing comprehensive staff codes of conduct. Staff who input into Mosaic are easily identifiable when they access or use the system. There will be routine audit of user access.	Reduced	Low	yes
Privacy intrusion and unexpected sharing	Additional information added to the top of the CAF form which clearly states what will happen and refers are responsible for telling people about it. Privacy notices for both the Tavistock and Portman NHS Foundation Trust and the Local Authority are updated, detailing the sharing of information across both services. It is accepted that there will be privacy intrusion but this is considered proportionate in respect of the benefits gained. It is noted that LB Islington has a similar system and have had no adverse findings etc from the ICO.	Reduced	Medium	Yes
Data Breaches	All partners have existing comprehensive data security policies, processes and procedures, and virus software etc are kept up to date. Staff with access to data will be appropriately trained in data protection requirements and there are existing comprehensive staff codes of conduct.	Reduced	Low	Yes

	Referrals will be made by email which are secure. Whilst breaches can never be fully eliminated, the parties believe this risk is mitigated as far as is possible.			

Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*
Medium

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	
Information Asset Owner acceptance of residual risks	Rashida Baig, Director of Children's Safeguarding and Social Work
This DPIA will kept under review by: (*usually the author or the IAO)*	[redacted]

Version Control

Version	**Reason**	**Date**	**Author(s)**
1.0	Final first draft	December 2022	[redacted] and Sarah Laws

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