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 health and care mental health day opportunities**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	
	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.*	A new integrated health and care mental health day opportunities model. The new service will be namely based at the Greenwood Centre forming part of Camden Council's Provider Services in-house mental health day service. The service will focus on providing more flexible support, meeting individual needs, connecting better with other local mental health services and improving access to mental health day support for Camden residents. Care and support will be provided by staff from Camden Council and C&I. A wide range of daily activities available. Individual weekly programmes will be co-designed with key workers. People will be able to draw upon the whole offer as and when needed. The clinical led element of the new offer will be staffed by clinicians seconded from C&I. Clinical interventions to be provided by C&I include: • Psychiatric assessment and treatments aligned with NICE guidelines	

	• Physical healthcare assessments, including ECG and bloods. • Psychology groups – e.g., Distress Tolerance Groups providing practical coping skills, coping with stress, art therapy etc… • Medication review and management The non-clinical element of the service will be staffed by a range of workers such as support workers, sessional workers as well as a dedicated social worker to support with Care Act Assessments which will be prioritised according to need for long term day support. Interventions will cover broad areas such as practical support (such as welfare rights and benefits), social and community groups (such as day trips, group movie trip, events), life and recovery skills (such as IT groups, coping skills, budget management, self-care) and physical activity groups (walking groups, gym, sports).
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Aimed start date of April 2024

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

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

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

Step 2: What personal data is being used?											
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New/Changed				
							Changed use				
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate										
	Personal Data										
	Name	**x**	Date of Birth	**x**	Gender	**x**	National Insurance Number		Financial Information about the person		
	Address	x	Email address	x	Telephone number	x	NHS No	x	Other eg a reference number such as Mosaic ref	x	
	Other data *(Please state)*:										
	Special Categories of Personal Data										
	Racial or ethnic origin	x	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion						
	Trade Union membership		Physical or mental health or condition							x	
	Sexual life or sexual orientation	x	Housing records Social services records		Tax, benefit or pension records		Employee/HR records				
	Other data *(Please state)*:		Mental health diagnosis and medications								
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?		Potentially – risk assessment could be logged								

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!**	Casework data on peoples mental health and support needs will be collected in order to inform the right kind of support to be provided. People who are within the service who are under the care of a secondary care/ core team will have details of their mental health on the Camden & Islington NHS Trust (CIFT) 'Rio' shared casework system. There may be some requirements for people who are being seen by the social care / Provider services part of the service whereby their notes from RIO need to be reviewed.
3.2	**Explain in as much detail as possible why this is being done**	With the changing profile of service user needs, recent expansion in crisis services and progress made towards implementing the Community Mental Health Framework, the plan is to provide a new type of Mental Health Day Support Service which is better integrated with other local services and will: • Address service gaps which currently exist in Camden, including the need for place-based intensive time-limited support outside of hospital for people experiencing acute mental illness • Progress the commitment shared by C&I and Camden Borough partners to advance joint working and improve integration of services at the 'PLACE' level. • Retain elements of the old ADU which local research shows result in better outcomes in terms of service user experience and satisfaction • Provide an alternative to hospital-based care and treatment for acutely unwell service users who would benefit from a place-based day program

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

- Maximise access and links to wider community support
- Provide a more streamlined pathway to reduce duplication, multiple assessment points, and a better understanding of people's support needs
- Improve alignment with community teams, the crisis pathway including the Crisis Sanctuary and MHCAS, the Resilience Network, individuals' existing support networks and wider community assets
- Improve integration/ alignment with longer-term support day opportunity services (Greenwood Mental Health Service and Phoenix Wellbeing and Recovery Service).
- Achieve efficiency and reduce duplication in overall provision by further aligning overlapping and complementary offers into an accessible referral pathway within the overall borough mental health offer

</td></tr>
<tr><td>3.3</td><td colspan="2">Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td>Yes/No</td></tr>
<tr><td></td><td>External organisation or partner Name</td><td>Controller or Processor?</td><td>Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? Yes/No/In progress</td></tr>
<tr><td></td><td>Camden & Islington NHS Foundation Trust</td><td>Controller (for information held within RIO)</td><td>There will be a Memorandum of Understanding between the Trust and the Council to cover various aspects of the agreement including the data sharing and data protection area</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

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.**	**Please see attached flow chart:**
3.5	**How will you handle data in your project, how will use store and share it. Please explain**	All data will be held within the C&I Trust RIO and related secure shared drive systems. Outcome monitoring data will be shared with LBC systems on an aggregate basis to inform quality of service and equalities monitoring.

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)(g) Processing is necessary for Reasons of substantial public interest (with a basis in law) and DPA18 schedule 1 Part 2 condition: para 18. Safeguarding of children and individuals at risk (h) Health or social care (with a basis in law) AND must specify one or more of: Data Protection Act 2018 Schedule 1 Part 1 condition: Paragraph 2	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Article 6(1)(e) public task - Data Protection Act 2018 Schedule 1 condition paragraph 2 health or social care purposes and paragraph 18. Safeguarding of children and individuals at risk. The underpinning laws for all are, the Care Act 2014 and the Mental Health Act 1983.

		Health or social care purposes and Paragraph 3 Public health The underpinning laws for all are, the Care Act 2014 and the Mental Health Act 1983.	
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 not required; code of conduct for access to service is signed (see HERE)		
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		
	This data is limited to what is relevant and adequate to complete the task.		
4.4	**Have/ will individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Privacy Notice? Remember telling people is not the same as asking for consent		Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**		
	The service will comply with council policies on Subject Access Requests and other data subject rights		
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?**		
	Each data controller will follow their own existing retention policies and procedures		

<table>
<tr><th colspan="2">Step 5: Information Security Process</th></tr>
<tr><td>5.1</td><td>On what systems will the data will be stored
Examples include Mosaic, SharePoint, shared drives,</td></tr>
<tr><td></td><td>C&I RIO system for patient casework information; C&I and LB Camden shared drives for other client related data</td></tr>
<tr><td>5.2</td><td>In what country is the data stored?</td></tr>
<tr><td></td><td>Data will be stored in the UK</td></tr>
<tr><td>5.3</td><td>What roles will have access to the information? (List individuals or staff groups)</td></tr>
<tr><td></td><td>LB Camden Provider Services Support and Key Worker roles, plus:

Clinician roles seconded in by CIFT: see below

<table>
<tr><td>Consultant Psychiatrist</td></tr>
<tr><td>Junior Doctor</td></tr>
<tr><td>Clinical Manager (supervision by Alice Murphy)</td></tr>
<tr><td>Clinical Psychologist</td></tr>
<tr><td>Art Therapist</td></tr>
<tr><td>Drama Therapist</td></tr>
<tr><td>Music Therapist</td></tr>
<tr><td>Exercise Therapist</td></tr>
<tr><td>Registered General Nurse</td></tr>
<tr><td>Registered Mental Health Nurse</td></tr>
<tr><td>Occupational Therapist</td></tr>
<tr><td>Additional management and IT costs (includes supervision from AM)</td></tr>
<tr><td>Mental Health Day Service Manager</td></tr>
</table>
</td></tr>
</table>

	Senior Support Co-ordinator Support Co-ordinator Recovery worker (TUPED) Senior Recovery Worker Business Support Officer Social Worker Service manager	
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**	
	The service will have role-based access controls. Only a healthcare or social care professional who is directly involved in a patient's care will be able to see that individual patient's record.	
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?**	
	RIO is secured with a login and password, and has access controls and auditing	
5.7	**Has the Information Security Team advised on the security measures? What were their comments?**	
	N/A	

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
***Misuse of data**; Personal data could be used in a manner incompatible with the Data Sharing Agreement. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.*	*Rare – all information will be shared via secure nhs.net / .gov accounts*	*Moderate*	*Medium/ high risk*
Compliance risk: could be a breach of purpose limitation and transparency	*Rare – all information will be shared via secure nhs.net / .gov accounts*	*Moderate*	*Medium/ high risk*
Corporate risk: Reputational risk. Loss of trust from data subjects and the partners providing the data. Legal implications.	*Rare – all information will be shared via secure*	*Moderate*	*Medium/ high risk*

	nhs.net / .gov accounts		
Personal data could be used in a manner incompatible with the Data Sharing Agreement. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.	Rare – there will be restricted access for roles to input and review data and a data sharing agreement shared	Moderate	Low

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?**
Corporate risk: Reputational risk. Loss of trust from data subjects and the partners providing the data. Legal implications.	Use of NHS.net/ .gov email accounts to ensure encrypted email system	Reduced	Minor / Moderate Risk	Yes
Compliance risk: could be a breach of purpose limitation and transparency	Training and appropriate policy. Data minimisation, sharing only what is needed.	Reduced	Moderate Risk	Yes
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Moderate / Minor				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	**No, Tanya Bryant Information Rights Officer**
DPO advice	
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			

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

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

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level*

	• Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

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

Table 4: is the risk level acceptable?

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

Appendix 2: Ethics screen.

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

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

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

-