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	**Parent Child Psychological Support programme – Camden Early Years Service**	
Project Lead and Information Asset Owner/s	Project Lead	Debbie Adams – Head of Integrated Early Years
	IAO name and asset	Steve Harris – Head of Facilities, for CCTV
	IAO name and asset	Debbie Adams – Head of Integrated Early Years for the data collected
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail.* E*xplain any acronyms on first use.*	This project, part of the service transformation in Camden Integrated Early Years, will increase the universal service offer for families with children in their first 1001 days (conception to age 2). The new service model includes the introduction of the Parent Child Psychological Support (PCPS) programme for Camden families. The PCPS programme was developed by Professor Cerezo, Chair of Psychology at the University of Valencia, who holds the property rights for the programme which focuses on supporting child development and the quality of the of the parent child relationship. The PCPS programme includes 6 clinic appointments for all children between 3 and 18 months during which a short 3 minute video recording of the parent playing with the child will be saved and then 'coded' to inform a discussion with a child psychologist. Further recordings are made at the 15 month clinic visit as part of the 'strange situation' test which is the accredited measure of attachment. The most suitable equipment for recording these interactions is CCTV as this allows 2 different views of the 'play' and allows the	

	practitioners to zoom in to better understand facial expressions. The CCTV cameras will be installed in a clinic room in each of the children's centre venues that will be hosting the programme. There are likely to be 5 venues in all. The cameras will be sued for the purposes of recording the parent child interactions as required in the PCPS programme and for no other purpose. Parents will give informed consent for the recordings to be made. The recorded interactions are analysed and 'coded' by the Psychology team at the Institute of Psychology for Children and Families (IPINFA) at the University of Valencia to inform the conversation with parents about their responses to their child and to support the quality of the parent-child relationship. (There is a separate DPIA that covers data sharing with IPINFA and other partners involved in the project). The aim is to support parents to respond sensitively to their babies' cues and signals, thereby developing a secure relationship in the early weeks and months of life. Studies undertaken in other areas that have offered PCPS show a marked improvement in the percentage of children who achieve a secure attachment by the time they are 18 months old. The programme is universal and will be implemented across Camden taking a **phased approach**. The objective is for all families to engage with the programme; the take up rates in other Countries that have run the programme (Spain and Ireland) have reached a 70% coverage. This DPIA covers the CCTV aspect only.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	The programme was launched in Camden at the end of June 2021 although, to date, only introductory visits and no filming has taken place. Roll out of phase 2, likely to be in Gospel Oak and Kilburn, is scheduled for March / April 2022, and phase three, Kentish Town East and Kings Cross in Autumn 2022.

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?)	Yes
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 have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	NO
1.6	Does the project involve multiple organisations, eg public sector agencies like 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?	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 physical harm in the event of a security breach?	NO
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					
							NEW					
2.2	**What data will be processed/shared/viewed?**											
	Personal Data											
	Name	**√**	Date of Birth	**√**	Gender	**√**	National Insurance Number		Financial Information about the person			
	Address		Email address		Telephone number		NHS No		Other eg a reference number such as Mosaic ref			
	Other data *(Please state):*	CCTV footage of parent and child, including zooming in on facial expressions of both										
	Special Categories of Personal Data											
	Racial or ethnic origin	√	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					√		
	Trade Union membership		Physical or mental health or condition							√		
	Sexual life or sexual orientation		Housing records Social services records		Tax, benefit or pension records		Employee/HR records					
	Other data *(Please state):*	These are not the primary data being recorded, and racial origin/religious beliefs/disability will only be incidentally processed for example where someone wears religious clothing, or a disability is visible.										
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	NO										

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data**	The recording of the parent / child interactions on CCTV are part of the PCPS programme. They are used to assess the attunement of a parent's responses to a child's cues. The recording will be assessed by a maximum of 5 named IPINFA psychologists who will access the material in the MS Teams site established for this purpose to which the psychologists will be granted 'guest' accounts. Guest account access will be managed by Business Manager and any amendments will require authorisation of the Early Years' Service Operations Manager. It is intended that CAHMS psychologists who are contracted to Camden will train to 'code' the video in due course removing the need for external user access.
3.2	**Explain in as much detail as possible why this is being done**	The DPIA that was completed prior to the implementation of PCPS sets out the benefits of the programme in full. In summary, the programme has been shown to increase the percentage of children that achieve a secure attachment to their principal care giver (usually the mother) by the time they are 2. The reason for making recordings is to allow the PCPS project to operate effectively. The attunement of parental responses to the child cannot be assessed by the PCPS programme experts unless they can see them. Viewing in real time is not possible and would be more privacy intrusive. The experts need recordings to be able to view and review and code as needed. Handheld recording was initially considered but was unviable due to technical operations. CCTV was fund to be the only technologically possible solution.

3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes
	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**
	IPINFA	Processer	YES – there is a contract and a DPIA for the implementation of the programme.
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		Yes, part of the PCPS DPIA
3.5	**How will the information be processed/shared. Details eg secure file transfer**		The data will be accessed through 'guest' access to a MS Teams account

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (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 The processing by videoing parents and children, storing that, sharing with IPINFA, their processing of it, and discussions between parents and psychologists will be based on	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** The processing by videoing parents and children, storing that, sharing with IPINFA, their processing of it, and discussions between parents and psychologists will be based on	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Not applicable

	explicit informed consent under art 6(1)(a) and 9(a).	explicit informed consent under art 6(1)(a) and 9(a).	
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 Information Tights Team have advised this is appropriate**		
	The processing by videoing parents and children, storing that, sharing with IPINFA, their processing of it, and discussions between parents and psychologists will be based on explicit informed consent under art 6(1)(a) and 9(a). Parents will be asked to sign a consent form when they join the programme.		
4.3	**How will you ensure data quality and data minimisation?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		
	Data quality is not applicable as it is footage that is being captured. For data minimization, the footage is only of the interactions between parent and child for the purposes of the programme. Parents will consent to this. The whole interactions of parents with health visitors etc is not recorded, just this one parent child set of interactions. The data collected as part of this project will be added to the child health record held on Systm1. Much of the information recorded will be the same as that collected and stored as part of the current health visiting service. The video footage will be held on the PCPS-Early Years Teams site hosted by the council. The video footage is additional data and will be used only to inform a conversation with parents about the relationship with their child.		
4.4	**Have 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 Processing Notice online		Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**		
	Yes		
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?**		
	Data will be retained and destroyed in line with the council's retention policy. IPINFA will not retain		

	personal data. The Tavistock and Portman NHS Foundation Trust, who employ the psychologists working in the PCPS team, will retain psychologist records in line with their retention policies which are acceptable to the council. The video recordings will be deleted after a period of 6 weeks.
Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*
	Data will be recorded by CCTV camera, connected to a Camden laptop and then uploaded by the programme administrator to the dedicated Camden Early Years Service MS Teams site.
5.2	**Where is the data stored geographically?**
	On a Cloud based MS Teams site.
5.3	**What roles will have access to the information?** (list individuals or staff groups)
	Practitioners within the PCPS team: • Health Visitors • Child Psychologists • Camden's IT support team where necessary
5.4	Is there role based access control on all applicable systems? **How will access to information be controlled?**
	Yes, access to the MS Teams Site will be by 'Guest' account managed by the councils early years service.
5.5	**Is there an ability to audit access to the information?**
	Yes, access to data will be overseen by managers within the service.
5.6	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories data and/or criminal data?**
	There is Role Based Access Control for all access to CCTV. For PCPS defined roles will have access and this will be auditable. The CCTV will be subject to the same security measures as the council's general in building CCTV
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**

	The information security manager has cleared the PCPS project as a whole. The CCTV is under the remit of the CCTV lead who has advised on appropriate equipment and usage.

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**
1. CCTV is inherently privacy intrusive and this is particularly intrusive in that it will be targeted footage of parent and child.	Likely	Moderate	12
2. The CCTV cameras remain operational at all times. This means that any use of the room in which the cameras are located could be recorded.	Likley	Moderate	12
3. A breach of security would allow footage of parent and child to be accessed by unauthorised people, causing intrusion and distress	Unlikely	Moderate	6
4. Relying on consent as a legal basis means parents have the right to withdraw from the programmeand therefore requiring CCTV footage to be deleted which may cause technical difficulties and cause delays in actioning erasure requests	Unlikely	Moderate	6
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 IRT/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?**
1.	Inherent privacy intrusion : the legal basis is explicit informed consent, so parents have a genuine choice about taking part or not. All CCTV will be signed and parents will be aware of when filming begins and ends having consented to the session. This makes the footage appreciably different from other CCTV footage.	Reduced	3	Yes
2.	Recordings will only be made of small sections of clinic visits for which parents have given consent. Notices will be placed at the entrance to the room informing parents and staff that cameras are present in the room but that recording will only take place as described in the consent form. The monitor will be placed in an office only accessible by PCPS staff. A notice will be placed on the monitor stating that it can only be used to view and record sessions as specified on the consent form. If the monitor is switched off the CCTV cannot be seen, and cannot be recorded.	Reduced	3	Yes
3.	Security breach. The CCTV is under the control of the council's CCTV manager and will be approved equipment that conforms to the council's required standards.	Reduced	3	Yes

4.	Effecting data subject rights erasure requests in a timely manner. CCTV systems retain footage for 30 days only, so any routine deletions would occur within a month of obtaining footage. Any erasure requests that were difficult to action would be implemented by routine disclosure.	Eliminated	n/a	Yes
Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*				
Moderate				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	**Sarah Laws**
DPO advice	I am happy with this processing. Andrew Maughan DPO and Borough Solicitor
Information Asset Owner acceptance of residual risks	Steve Harris – Head of Facilities, for CCTV Debbie Adams – Head of Integrated Early Years for the data collected
This DPIA will kept under review by: (*usually the author or the IAO)*	Debbie Adams

Version Control

Version	**Reason**	**Date**	**Author(s)**
1.0	New DPIA	Aug 2021	Debbie Adams and Sarah Laws
2.0	Amended for changes to CCTV	October	Debbie Adams 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

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) This will be a link to Camden's Data Charter but this does not exist yet

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?*

-