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	EyMan Nursery App Video Recording Implementation	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Debbie Adams, EyLog smartphone app
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.*	The Integrated Early Years Service Nurseries are moving from paper-based record keeping to an online information management system This information within the new nursery information management system, is held within 2 systems. EyLog smartphone app - This is of benefit to Camden residents, nursery parents, sharing their child's learning journey, demonstrating how children are spending their day in the setting. This may include video/audio recording and photographs, via EyLog App - This is sharing the nurseries Early Years Foundation Stage records including children's educational assessment by observation and progress with parent of nursery children Background information a) EyLog and EyMan database form the nursery management information system - See separate DPIA for EyMan The nursery staff use tablets in the nursery rooms to share photos and videos to evidence children's learning. This then can be shared with parents via the EyLog app. The nursery staff are given training and guidance on GDPR and confidentially before being registered	

	within the EyLog database. Staff permissions are managed by the data and performance team
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Ongoing - A pilot is taking place in Hampden and Harmood nurseries, no information has been shared to date, but staff have trained

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 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?	no
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 compare privacy regulation?	no

<table>
<tr><th colspan="12">Step 2: What personal data is being used?</th></tr>
<tr><td>2.1</td><td colspan="8">Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?</td><td colspan="3">New/Changed</td></tr>
<tr><td></td><td colspan="8"></td><td colspan="3">New - formally paper photos were used, now moving to digital photos</td></tr>
<tr><td>2.2</td><td colspan="11">What data will be processed/shared/viewed?
-</td></tr>
<tr><td></td><td colspan="11"><u>Personal Data</u></td></tr>
<tr><td></td><td>Name</td><td></td><td>Date of Birth</td><td></td><td>Gender</td><td>yes</td><td>National Insurance Number</td><td></td><td>Financial Information about the person</td><td></td></tr>
<tr><td></td><td>Address</td><td></td><td>Email address</td><td></td><td>Telephone number</td><td></td><td>NHS No</td><td></td><td>Other eg a reference number such as Mosaic ref</td><td></td></tr>
<tr><td></td><td colspan="3">Other data (Please state):</td><td colspan="8"></td></tr>
<tr><td></td><td colspan="11"><u>Special Categories of Personal Data</u></td></tr>
<tr><td></td><td>Racial or ethnic origin</td><td>yes</td><td>Fingerprints/ Biometrics</td><td></td><td colspan="6">Religious or philosophical beliefs Political opinion</td><td></td></tr>
<tr><td></td><td>Trade Union membership</td><td></td><td colspan="7">Physical or mental health or condition</td><td>yes</td></tr>
<tr><td></td><td>Sexual life or sexual orientation</td><td></td><td>Housing records Social services records</td><td></td><td>Tax, benefit or pension records</td><td></td><td colspan="3">Employee/HR records</td><td></td></tr>
<tr><td></td><td colspan="3">Other data (Please state):</td><td colspan="8">None</td></tr>
<tr><td>2.3</td><td colspan="3">Will it include data about any criminal offence committed or alleged, or criminal offence record?</td><td colspan="8">n/a</td></tr>
</table>

<table>
<tr><th colspan="4">Step 3: Describe the data processing</th></tr>
<tr><td>3.1</td><td colspan="2">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 trnsfered/shared?</td><td>The child's learning journey is digitally shared with the authorised parent/carer via an app. It is only shared with the parent/carer.
EyLog is a tablet-based system accessed by users through either an Apple iPad (minimum Apple operating system version 9.0 or above) or Android (minimum Android operation system version 4.0 or above) tablet which have WiFi capability</td></tr>
<tr><td>3.2</td><td colspan="2">Explain in as much detail as possible why this is being done</td><td>Sharing a child's learning journey digitally increases the parents' involvement in the activities at the nursery. The system incorporates photos, videos, and audio. It helps the parent to have an immersive experience of what a child is learning at the nursery and the context in which the child is engaging in various activities, encouraging their overall growth and development. The advantage is that parents can receive up to date information in real time.</td></tr>
<tr><td rowspan="4">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>No apart from the service provider</td></tr>
<tr><td>External organisation or partner
Name: EyMan</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</td></tr>
<tr><td>EyMan</td><td>Processor</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>3.4.</td><td colspan="2">Has a data flow mapping exercise been undertaken?
If yes, please provide a copy, if no, please undertake</td><td>No – none required</td></tr>
<tr><td>3.5</td><td colspan="2">How will the information be processed/shared. Details eg secure file transfer</td><td>The information is shared securely from Camden's secure IT system to EyMan app</td></tr>
</table>

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 Article 6(1)(a) consent- parents/carers will consent on behalf of the child who will be too young to provide their own consent	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9(a) explicit consent - parents/carers will consent on behalf of the child who will be too young to provide their own consent	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Not applicable
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 Rights Team have advised this is appropriate**		
	The IEYS require all parents to read, understand and sign the information checklist as part of the registration process, this identifies parent permissions including, photographs, videos and sound recording and sharing. The permissions adhere to best practice around taking photos, videos, and audio of children, explaining how these will be used. All staff will be trained in these policies and procedures.		
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		
	Staff are trained in these policies and procedures which describes how to identify appropriate content to share		
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 current data retention policy. Please find attached Camden Children centre retention policy		

	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.*
	The software is provided as a cloud-based SaaS platform hosted on AWS servers located at data centres in London. EyMan is a web-based system accessed by users through a web browser with no additional hardware requirements, while EyLog is a tablet-based system accessed by users through either an Apple iPad (minimum Apple operating system version 9.0 or above) or Android (minimum Android operation system version 4.0 or above) tablet which have Wi-Fi capability
5.2	**Where is the data stored geographically?**
	The software is provided as a cloud-based SaaS platform hosted on AWS servers located at data centres in London.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Senior management staff (IEYS), Nursery staff, centre head, deputies and seniors
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	The system allows for permissions to be set, so not all staff can access all areas of the system
5.5	**Is there an ability to audit access to the information?**
	Yes, there are access reports available
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?**
	The staff members that can access the data will be aware of all aspects of data protection and they are also all DBS checked. The staff accessing the data will be given log ins and will only be given access to the data that they need to be able to do their job. With parents we will discuss with them Camden's polices around data sharing but do note that we would be unable to stop them if they wish to share the data on their own personal social media outlets
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	The security team were part of the procurement process and signed off the project

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 – a member staff could share photos/video inappropriately, leading to privacy intrusion and misuse of data for nefarious and illegal means by a third party. It is noted that this is data of small children who under GDPR are afforded special protection data protection wise.	Possible	Major	Medium/high
Consent is not properly informed, leading to processing have no lawful basis. This is a risk given it is children's data and the possibility of disputes between parents or parents and the council for LAC	Possible	Major	Medium/high
A staff member is not carefully about removing or blurring out another child – privacy intrusion, data shared with 3rd party without consent, possible harm as misuse of data above	Possible	Major	Medium/high
Information regarding a Looked After Child (LAC) is disclosed inadvertently, by a deletion or blurring failure as above. LAC are highly vulnerable and disclosure to a 3rd party could cause widespread harm.	Possible	Major	Medium High
Photos/video uploaded to wrong child's account meaning wrong parent/carer access the data with privacy issues and risks as other risks above.	Possible	Major	Medium High
Data retained beyond retention period leading to information being held for too long	Possible	Major	Medium High
Parents/carers allowing 3rd parties access to data about their children resulting in intrusion or harm	Possible	Major	Medium High

Failure of security controls resulting in data breach and data being exfiltrated	Possible	Major	Medium High
Inherent privacy intrusion caused by videoing/photographs	Possible	Major	Medium High

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?
Misuse of data – a member staff could share photos inappropriately	Member of staff would have to set up a false account, but any account that is set up must be authorised by a senior member of staff so the risks are reduced. Staff members have enhanced DBS checks and there are policies and procedures in place. The database is overseen by the data and performance team and the locality leaders. This allows the database to be overseen by a team that do not work directly in the children centres. This team also oversee several other databases within IEYS. We can create a series of reports that allows us to track staff usage	Minimise risk	Moderate	
Consent issues	Consent forms will be appropriately drafted and staff trained to ensure that consent is freely given. Where there are disputes between parents or carers, or between parents/s and the council for a LAC, a cautious approach will eb taken, where a refusal of consent overrides consent from other parent/s/carer/s etc.	Minimise risk	Low	

A staff member is not careful about removing a child- LAC or not	Ongoing training and reminders. Also, a policy guidance that instructs staff that they only share videos showing one child and make sure there are no children visible in the background	Minimise risk	Moderate	
Uploading to wrong child's account	Before any photos or video are sent to a parent, these must be approved by either the head of centre or key worker. If there such a incident the centre head would inform the parents and then as the video etc goes through app, the data can be deleted and is recoverable.	Minimise risk	Moderate	
Data retained beyond retention period	We have a data retention document that is part of the induction and training for all children centre staff. We will run regular reports to ensure that children's data is not kept beyond the retention date. The data team already oversees the deletion of records from the EISi database so have procedures in place for delating child's records	Minimise Risk	Low	
Improper parental actions	Once the data is accessed by parents, the council's responsibility, in law, ends. Parents are not subject to GDPR and actions they take are their own responsibility not the council's. However, the council may have reputational damage from parents improperly using data and where parents have improperly used personal data they have been given inadvertently by the council (eg an upload to wrong child's account) the council may have liabilities for the breach in improper uploading. The key workers/centre heads will enter in discussion with parents before they have access to the app. We will set out the policies and procedures in have in place regarding the use of the app. We will ensure parents are informed if there are any issues e.g., wrongly uploaded data that they have relevant contact details e.g., centre	Removed- not Camden as a data controller	None	

	head where this matter can be reported. Also, they would be advised that they must delete data if it was wrongly sent to them			
Failure of security controls	Whilst these can never be fully guarded against the system has robust controls in place which have been deemed acceptable by the council's Information Security Team	Minimise Risk	Low	
Inherent privacy Intrusion	The consent will be provided by parents/carers as the children will be too young to provide their own consent, and it might be considered they would be too young to realise any intrusion. However, as data subjects in their own tight, the fact they have no agency ought to be noted, although given the purposes of the recording, and that it is provide to parents/carers only, with the safeguarding above it is considered that any intrusion is minimal and proportionate.	Minimise	Low	
Residual (remaining) risk level when all mitigations have been applied:				
Medium -Debbie Adams				

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	Debbie Adams
This DPIA will kept under review by: (*usually the author or the IAO)*	[redacted]

Version Control

Version	Reason	Date	Author(s)
1.0	New DPIA	May 2022	[redacted] Sarah Laws

Appendix 1- deleted

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) 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?)*

- We can share a child's learning journey digitally with increases the parents' involvement in the activities at the nursery. The system incorporates photos, videos, and audio. It helps the parent to have an immersive experience of what a child is learning at the nursery and the context in which the child is engaging in various activities, encouraging their overall growth and development

b) *What would be the harm in not processing this data?*

- Parents will not have access in real time to their children's activities when at the nursery

2. *Data Bias*

a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?*

- The IEYS require all parents to read, understand and sign the information checklist as part of the registration process, this identifies parent permissions including, photographs, videos and sound recording and sharing. The permissions adhere to best practice around taking photos, videos, and audio of children, explaining how these will be used. All staff will be expected to be familiar with these polices

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?*

- We will resolve errors promptly. Revising practice, policies, and procedures as necessary as part of our commitment to continuous improvement.

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**? Children whose images have been incorrectly shared. Parents are very clear about what data is being shared and how it will be used.

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?*

- Children where permission is not granted can be ammonised, this is a function of the software. Sharing of videos would be strictly and carefully managed. Staff will be very clear on what is shared digitally and what we do not share.

*b) How are you ensuring the data used is reliable? (**Data quality**)*

- *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*
  - *n/a*

- *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)*
  - n/a – This is a closed system that centres around running a nursery. The data only is collected for this purpose.

d) *How could the objectives of this project be completed without processing the data?*
  - We would be unable to communicate in a digital way with parents so they would be unable to be involved in the immersive experience of what a child is learning the nursery.