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	**SEN Mini buses with CCTV**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Sam Pandya, CATS vehicle CCTV system
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.*	Use of internal and external CCTV in vehicles used by the CATS team to transport children with SEN. 12 new compressed natural gas (CNG) vehicles have been purchased from Nu-Track, Ballymena, Belfast, which have internal and external CCTV installed. Each vehicle has: 3 internal cameras – 1 facing the entrance door, 1 at the rear covering the passengers, 1 on dash facing forwards covering the road 2 external cameras – located at top front corners facing rearwards covering the road and length of vehicle.	

	All cameras are video only with no microphones fitted (so no sound is being recorded). This is a standard amount of cameras for this vehicle type. All vehicles have signage stating 'CCTV in operation' These are fitted to assist the protection of Special Educational Needs (SEN) children being transported, drivers and personal assistants (PAs) from any allegations, as well as to capture any driving infringements either fault or non fault. The manufacturers are Journeo (formerly 21st Century), CCTV - Journeo. Footage can only be viewed once extracted from the local hard drive and cannot be viewed remotely. Footage only to be downloaded in event of an incident, allegation of driving or criminal offence. Protection of SEN passengers, driver and external pedestrians, cyclists, road users. The request must be made in writing i.e. email and sent to CCTVPatrols@camden.gov.uk accompanied by a completed and authorised Employee Monitoring Form request where the request will be authorized dependent on justification for reviewing and the engineering manager will be provided with a request CCTV URN (unique reference number) associated to the request. CATS CCTV request form to be completed with reason for request and only to be downloaded by Engineering Manager
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	5th October 2021 (backdated)

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	Yes
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 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	Yes	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							
	Special Categories of Personal Data									
	Racial or ethnic origin	Yes	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion			Yes		
	Trade Union membership		Physical or mental health or condition					Yes		

	Sexual life or sexual orientation		Housing records Social services records		Tax, benefit or pension records		Employee/HR records	
	Other data *(Please state):*	Behaviours of those recorded which may include special category data.						
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	If the footage captures an alleged offence- whether driving or personal etc then 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?**	The footage is created as the vehicle is in use. If there is no incident then the footage will be retained for the retention period and then deleted and so not accessed. The footage will only be accessed- as below and elsewhere in the DPIA- when authorised and to investigate an incident. Data images/footage will only be downloaded in event of an incident with either the vehicle or an individual on board.The request must be made in writing i.e. email and accompanied by a completed and authorised Employee Monitoring Form request and sent to CCTVPatrols@camden.gov.uk where the request will be authorized dependent on justification for reviewing and the engineering manager will be provided with a request CCTV URN (unique reference number) associated to the request. The engineering manager will then [redacted], data cable plugged into the hard drive, which is held by the engineering manager, the data is encrypted so only able to be viewed by using specific software which is only installed on the engineering managers laptop which is password protected, and copied from the hard drive only by the Engineering Manager. CCTV request form to be completed by authorised Manager (Logistics Manager and Head of Service). Footage to be held on the Engineering Managers laptop which is password protected held only by the Engineering Manager. If footage is requested this will be emailed in an encrypted folder with password sent separately.

3.2	**Explain in as much detail as possible why this is being done**		Protection for the driver and council regarding any driving infringements, accidents, or allegations toward the driver/PA who are transporting children with SEN. To ensure that the children's safety is assured. Many of the children will be unbale to explain any incidents or concerns and so CCTV will provide evidence of whether an incident occurred or not. If a SEN child has acted in a way that has caused harm to themselves or others the CCTV footage will provide proof of what occurred.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes/~~No~~ in the event of an incident, either driving or other, footage has potential to be required to be shared with Police and insurance companies,. Potential in the event of national emergency for security services to request footage of vehicle in the area for any possible evidence.
	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~~**
	Met Police	Controller	Existing suite of DSAs to cover crime and safeguarding sharing

3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**	Yes/~~No~~
3.5	**How will the information be processed/shared. Details eg secure file transfer**	The footage is created as the vehicle is in use. If there is no incident then the footage will be retained for the retention period and then deleted and so not accessed. The footage will only be accessed- as below and elsewhere in the DPIA- when authorised and to investigate an incident. Any footage extracted by the Engineering Manager, only with the consent of the CCTV team, can only be viewed on the Engineering managers laptop which is a password protected Camden asset. Sharing of any footage is to be done only with express consent of CCTV Data and Governance Manager

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)(e) public task and article 6(1)(c) legal duty with the underlying law for both being that as per article 9	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9(2)(g) public task with the Data Protection Act 2018 schedule 2 conditions being para 6 governmental purposes and	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** The article 10 requirements are met by the article 6 conditions and the DPA18 schedule being that met by special category data

		para 18 safeguarding with the underlying law for both being the Health and Safety at Work etc Act 1974, the Equality Act 2010, The Children Acts, and the Care Act 2014	
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Rights Team have advised this is appropriate**		
	Consent is not the legal basis		
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		
	Data accuracy is not applicable as it is CCTV footage.		
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/~~no~~
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?**
	Only data that is downloaded to be kept for a maximum period of 12 months once any investigation is completed. Data held on the hard drive is recorded over in a continuous loop and the max retention for this is 30 days.
	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.*
	Internal hard drive within vehicle, any footage downloaded will be stored in Engineering Manager's One drive in an individual folder and viewed on Engineering Manager's laptop. This is the only laptop with the 21st Century DVR Client viewer installed.
5.2	**Where is the data stored geographically?**
	Laptop One Drive cloud account of Engineering Manager
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Engineering Manager

5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Only Logistics Manager and Head of Service to request CCTV footage via email to be justified and then will be viewed on Engineering Manager laptop only
5.5	**Is there an ability to audit access to the information?**
	CCTV footage requests to be kept on Engineering Manager's laptop. All saved footage will have a corresponding request which will have been sent via email.
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?**
	Engineering Manager's laptop is password protected. Only requested footage by an authorised manager, once approved by the CCTV team, is to be downloaded and kept in secure folder. Engineering managers laptop in only unit in the business to have the required footage client. Any footage that is to be sent to be done within encrypted folder and only with permissions as detailed above.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Privacy intrusion caused by continual CCTV recording, loss of control over data, embarrassment distress. Data subjects are working so will record their working time, and the SEN children are inherently vulnerable.	Likely	Major	High Risk (16)
Misuse of data; footage downloaded unnecessarily and shared with staff not required to view resulting in harm, distress and intrusion.	Possible	Major	Medium High Risk (12)
Hard drive failure/camera damage – unable to view footage to support any incident/allegation. Accessibility breach.	Possible	Major	Medium High Risk (12)
recorded data obtained by unauthorised third party by inappropriate sharing	Possible	Major	Medium High Risk (12)

recorded data obtained by unauthorised third party by data breach	Possible	Major	Medium High Risk (12)
Downloaded Data retained past retention period by managers resulting in risk of disclosure, and privacy intrusion, as the deletion is a manual process	Possible	Major	Medium High Risk (12)

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?
Privacy intrusion.	CCTV notice in vehicles. Public are accepting of this type of CCTV.	Reduced impact.	Medium high	
Internal misuse of data	Staff all covered by employee code of conduct and relevant information governance and data security policies. Role based access control and authorisation process for access of data.	Reduced likelihood	Medium High	

Equipment related accessibility issue	Equipment sourced from established source. Drivers carry out daily first use and final use vehicle check which incorporates a check of the CCTV footage as viewed on the internal vehicle screen. Any damaged cameras or footage not available is reported to Engineering department	Reduced likelihood	Medium High	
Inappropriate sharing with 3rd party	Staff all covered by employee code of conduct and relevant information governance and data security policies. Role based access control and authorisation process for access of data.	Reduced likelihood	Medium High	
Data Breach	Equipment sourced from known provider. Which is secured using a lock and once removed is encrypted so only able to be viewed using specific software.	Reduced likelihood	Low	
Downloaded data kept beyond retention	Manager aware of requirements.	Reduced likelihood	Moderate	
Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*				
Medium High				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	Sarah Laws Data Protection Manager
DPO advice	This CCTV is standard practice now and is sensible subject to the safeguards which appear proportionate and adequate. Andrew Maughan Borough Solicitor and DPO May 2023
Information Asset Owner acceptance of residual risks	Sam Pandya May 2023
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted], Sam Pandya

Version Control

Version	Reason	Date	Author(s)
1.0	New DPIA	May 2023	[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

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 riskA number of control measures may be required

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

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?)* • Increased protection in case of any incidents involving the vehicle, passengers or members of the public. In the case of a national emergency then this provides additional support to security services. b) *What would be the harm in not processing this data?* • In allegations towards staff from clients this would be putting them at risk of either a false allegation or putting the client and any future clients at risk of staff acting not as trained.
2. *Data Bias* a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?* • n/a 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?* • n/a

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**?

- No one

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?

- Data is only extracted on the request of a senior manager in the event of an incident. Only information reported in the incident is taken into consideration unless there is risk to life.

*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**)*

- Cameras are checked daily by drivers to ensure they are not damaged and working during theirvehicle checks.

*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)*

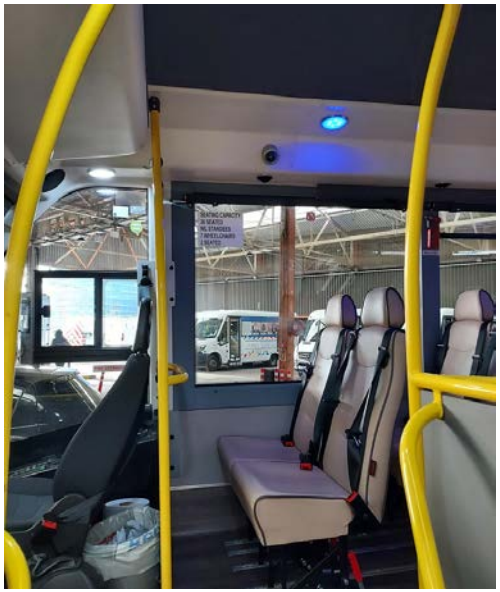
- Yes

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

- We would need to rely on verbal statements from individuals, which is not always accurate, rather than factual CCTV evidence.

Location of Cameras Fitted to vehicle:

Offside front internal – facing entrance door



Internal rear central – facing towards the front covering passengers



Internal drivers dash – facing road with monitor on right hand side



External nearside front upper – facing rearwards covering the road



External offside front upper – facing rearwards covering the road



Internal signage – on partition behind driver, facing passengers



Location of hard drive – [redacted]