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	**Processing Sensitive Personal Data by LaneWatch cameras**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Peter Mardell
	IAO name and asset	Parking Operations
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 DPIA has been submitted as an extension of Parking Operations existing DPIA that covers the use of unattended CCTV cameras ("LaneWatch"), and which was approved in the Summer of 2021. The reason for the additional submission is based on a possible change in the scope of where LaneWatch cameras may be installed in the future, which could now see these in streets or places where there are health centres, specialist clinics, GP practices, hospitals, and Police stations and the related processing of sensitive personal data for those places. This risk with this change in approach is that recorded footage may contain additional information which is more than was intended, but which could be used to identify a living person or infer conditions relating to that person's health, criminal record, and religious beliefs (aspects covered under the UK GDPR). It is also acknowledged that persons attending such places may do so in a vulnerable state, in distress, or under duress and while this may not be considered a material concern, there is a potential for shame, harm or self-harm to come about to the person because of information being made public. Given the potential seriousness of the situation, Parking Operations have sought to submit a sperate DPIA to explore these themes and risks in detail to ensure that a balance is achieved regarding the impact to privacy.	

Background

Article 4(1) of the UK GDPR defines personal data to mean any data which can be used to identify a natural living person. While data captured through CCTV cameras would not on its own be enough to identify a person, used in conjunction with other data source(s) such as the DVLA vehicle register and social media, it is possible to enable identification. Therefore, the provisions set out in the UK GDPR concerning personal data are engaged.

The lawfully processing of personal data by Camden is made possible by Article 6(1)(e) of the UK GDPR which reflects the role of the council as a "traffic authority" within the context of the Road Traffic Regulation Act 1984 (RTRA) and the Traffic Management Act 2004 (TMA). This status gives Camden cause and appropriate authority to make use of the DVLA's KADOE system, under licence, for the purpose of issuing a Penalty Charge Notice (PCN) under those regulations.

Personal data in relation to health is covered under Article 4(15) which provides the definition, Article 9(1) which prohibits the processing unless specific conditions are met, and Article 9(2) items (e), (f) and (g) which set out our legal basis for processing this information in the pursuant of our legal powers.

As Camden is not processing "sensitive information" directly through this project, rather we are exploring a change in camera deployment, we become aware of this information indirectly:

- Whereby a person(s) volunteers it in respect to a PCN appeal; or
- Whereby the recipient of the PCN publicly discloses the information and a person is identified through the disclosure (online witch-hunt).

This configuration would support that placing LaneWatch cameras near community health centres, places of worship, or police stations may be construed as acceptable where it relates exclusively to Camden's powers under the TMA and RTRA respectively, and where the processing of special category data is not intentionally but incidental.

There are some additional concerns related to the scope of activities and persons who have cause to attend police stations:

- Persons who are victims of crime or perpetrators attending.
- Persons who support victims of crime or provide legal aid attending.
- Persons who have temporary immigration status and who are required to register with a police station.
- Persons who are classified as 'registered offender' and who are required to register with the Police station.
- Persons who are involved in undercover work or national security, and for whom secrecy of their identity is imperative for their work and safety.

	In this setting, persons may be inadvertently identifiable due to external factors outside of the control of Camden i.e. persons public profile, any public information made public by the police through an appeal, newspaper stories (including online) or similar disclosures about persons. The risk here is that while the cameras would be configured against the relevant traffic restriction or prohibition, it is possible for recorded data to include additional information (depending on the specific camera view). This is particularly a risk with any camera fitted with a wide-angle lens, and where the view cannot be manipulated to completely remove any unnecessary information from the background imagery. Here, a person who is reviewing the footage may observe events or persons who are not related to the traffic contravention. This may include persons seen attending specialist health clinics or being arrested and transferred in restraints to police station which allude to health conditions and criminal records. Depending on the depth of field (view) of the camera it may be possible to identify a person(s) using this information, more so if the person is known to the reviewer or where additional data sources are used in conjunction with the footage to identify the person. Similarly, a person may volunteer this information to Camden as part of an appeal against a PCN. If this information is made public through social media, it could have some indirect consequences for the identified person(s) in the sense of causing them harm either physical or mental.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	TBC – ETA Q2 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?)	
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	
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?	
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?	
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 ?	
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?	
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	
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?	
1.9	Will data be combined, compared or matched from multiple sources?	
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	
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?	
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	
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?	

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**			
							The processing of personal data by LaneWatch cameras is already happening. This is a change in the potential scope of data that may be processed, which may now include "sensitive personal data" due to proximity of cameras to community health centres and police stations. It should be noted that the camera does not process this data, but rather this is a subsequent, indirect, result of the camera having captured data in the first instance.			
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):*			The vehicle registration mark (VRM) is the only personal data that will be processed directly through the cameras. Externally to the project, once a PCN has been generated, it will be posted to the "registered keeper" (owner) of the vehicle at the time of the contravention, as advised by the DVLA.						
	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):*	No sensitive personal data will be directly processed by the LaneWatch cameras, either at the point of capture or when the data is being reviewed by a CEO. The processing of sensitive personal data will only be known by Camden indirectly (outside of this project) after a PCN has been posted to the registered keeper of the vehicle, as confirmed by the DVLA for such purposes, and where that person appeals against the PCN and discloses such information willingly for the purpose of Camden withdrawing the PCN. In some cases, Camden may request evidence of such to support any purported claims from the person.						
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	**No.** The camera product has been constructed and programmed to only capture data in relation to the breach of the relevant traffic contravention by motor vehicles and will not by default collect any data outside of that convention. However, in a purely hypothetical sense, it may be possible for captured data (footage) to show background incidents of lawbreaking, civil disobedience, anti-social behaviour, or persons being stopped and/or arrested at the scene by Police, including person being escorted into police station(s) in restraints, where these to fall within the camera's field of view at the exact same time of the contravention occurring (a 'compound event' in essence). Furthermore, it may be possible that the recipient of the PCN could recognise the person(s) in the footage or make an unauthorized copy of the footage and post it on social media, online forums, file-sharing sites, or similar which in turn could result in a person(s) being identified through an online witch-hunt. Parking Operations holds no data on the probability of such an event taking place (although it is believed to be low due to the series of events which would need to occur) and has been provided here for transparency purposes.						

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?**	No change from the previous DPIA. In summary: 1. **Point of Capture**: The camera will identify a contravention using onboard VCA software and will capture the relevant data for review (normally a 15 second video clip and ANPR image of the VRM). The data is sent wirelessly and securely to a server where it will be stored until the clip is reviewed. 2. **Post capture**: CCTV Supervisors will allocate the captured data for review by a CEO using back-office CCTV software ("Metro"). 3. CEOs who have been allocated captured data for review will view the footage and determine whether a contravention has occurred. There are two outcomes here: a. If the captured data does not confirm a contravention has occurred, the data will be rejected and purged from the server. b. If the data does confirm a contravention has occurred, the data will be further processed into a PCN. In practice this means, the CEO will visually review the data and will undertake the following actions: i. Record the VRM from the footage. ii. Record the data and time of the contravention. iii. Record the location the contravention has occurred. iv. Select the appropriate contravention code. v. Produce between three to five images from the video footage which confirm a contravention has occurred. vi. Issue a PCN. The data will be exported with all assigned values and images to Camden's Parking Management System

		("Taranto"), when a PCN will be generated from the data. vii. At the conclusion of this process a unique reference number for the PCN will be generated against the captured data. viii. The CEO will produce a Witness Statement entry for the contravention / PCN for audit purposes. This will be stored in line with our retention plan before being destroyed. ix. The data having been reviewed will now be transferred from the review queue and stored on the archive server and retained in accordance with the data retention plan. This effectively, concludes data processing for the project
3.2	**Explain in as much detail as possible why this is being done**	Camden is pursuing this project to allow it to undertake a wider spectrum of monitoring including outside sensitive places for the following purposes: • To manage traffic on our road networks to ensure, as reasonably possible, the expeditious and safe movement of persons, vehicles and goods as part of our network management duty under section 16 of the Traffic Management Act 2004 and section 122 of the Road Traffic Regulation Act 1984 respectively. • Local authorities have a statutory duty to improve local road safety and "take (reasonable) steps to reduce and prevent accidents" as required under section 39 of the Road Traffic Act 1988. • To support Camden's "public sector equality duty" in relation to making the

<table>
<tr><td></td><td></td><td></td><td>highway more accessible by persons who are disabled under the Equality Act 2010. This will be delivered in part by removing dangerous and inconsiderate driving and parking by motorists.
• To support and deliver local environment and sustainability objectives as set out in the Camden Plan 2025 and the Camden Transport Strategy respectively.
• To support aspects of the London Mayor's 'Transport Strategy 2018' and the 'Vision Zero Action Plan' which aim to reduce pollution, improve air quality and accidents on roads in London.
Collectively, the above will be support using unattended cameras.</td></tr>
<tr><td rowspan="2">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
Camden will be processing data in line with the statutory processes set out in the Traffic Management Act / related statutory instruments and data sharing is limited between Camden, the registered keeper of the vehicle or person in charge of the vehicle at the material time (hire agreement) and the Enforcement and Traffic Adjudicators (ETA) for any PCNs which are appealed to the parking adjudicators.
Camden holds existing contracts for civil parking enforcement and CCTV support and maintenance which will have some interaction with the process on behalf of Camden:
- Marstons Holdings who provide CEOs to Camden
- Tyco who are incumbent CCTV maintenance service provider to Camden.</td></tr>
<tr><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>
</table>

	NSL Services Ltd / Marstons Group	Processor	**Yes**. An existing contract between parties for Civil Parking Enforcement services, which includes data-sharing, confidentiality, and data protection clauses and sub-agreements.
	Tyco Fire & Integrated Solutions Ltd	Processor	**Yes**. Existing contract for the provision, configuration, support and maintenance of CCTV cameras and associated equipment, including the LaneWatch product, that also includes data-sharing, confidentiality, and data protection clauses and sub-agreements.
	Siemens Mobility UK	Processor	**Yes**. There are existing contracts in place for CCTV services provided by Siemens to Camden which includes data protection, data-sharing and confidentiality requirements and clauses.
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**		**Yes**/No This has been provided under previous submissions.
3.5	**How will the information be processed/shared. Details eg secure file transfer**		Only limited persons will have access to the data, and this will be 'shared' via Camden servers. In respect to processing / sharing, the following: • The LaneWatch camera will capture data of alleged contraventions at the scene and will package this for transmission wirelessly to Camden servers. • The Camden servers are located within Camden network infrastructure, and sit behind industry standard protection e.g. firewalls, port filtering / blocking, RBACs, hardware and software keys and similar. • Incoming data is stored on a server pending review, and once completed archived on another for storing, in line with our data retention plan. • If the server(s) were to fail for whatever reason, Camden has suitable business continuity in place that aims to restore the data via system data recovery process and integrity testing.

<table>
<tr><th colspan="4">Step 4: Assess lawful basis, necessity, and proportionality</th></tr>
<tr><td>4.1</td><td colspan="3">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</td></tr>
<tr><td></td><td>Personal data:

UK GDPR Article 6(1)(e) performance of a public task by Camden in pursuant of statutory powers under the Traffic Management Act 2004 and Road Traffic Regulation Act 1984.</td><td>Special Category data:

UK GDPR Article 9(2)(g) reasons of substantial public interest with a basis in law, with the Data Protection Act 2018 Schedule 1 conditions, being paragraph 6, governmental purposes and the underlying law being the Traffic Management Act 2004 and Road Traffic Regulation Act 1984.</td><td>Criminal data:

N/A</td></tr>
<tr><td rowspan="2">4.2</td><td colspan="3">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</td></tr>
<tr><td colspan="3">N/A</td></tr>
<tr><td rowspan="2">4.3</td><td colspan="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</td></tr>
<tr><td colspan="3">The data captured by the camera will be directly related to the vehicle and the breach of the traffic regulation being monitored. It is generally a closed affair between Camden, the registered keeper of the vehicle and an arbitrator (ETA) in accordance with the requirements, processes, and procedures of the legislation.

Data accuracy will be maintained as the video footage cannot be edited. Once captured it will be transferred to a secured server where it will be preserved (read only) in line with our data retention plan.</td></tr>
<tr><td>4.4</td><td colspan="2">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</td><td>Yes, as far as reasonably possible. Unfortunately, it is not possible to identify in advance of time who will contravene traffic regulations and therefore no means to forewarn of the processing ahead of time.

Instead, appropriate on street traffic signs have been installed that advises of the restriction or prohibition, including where appropriate the use of advance warning notices, which conform to the Traffic Sign Regulations and General Directions requirements.</td></tr>
</table>

		These traffic signs will be known to motorists, as they are very common across the UK and EU but also covered within the Highway Code, and driving licence learning / examination processes. Furthermore, each camera installed on street will be accompanied by a sign which advises that Camden is the operator of the camera, its purposes, and our contact details should anyone which to enquire about the asset. Lastly, the scope of personal data processing under this project is set out in the Camden and Parking Operations privacy notices, which can be freely viewed on the Camden site. Collectively this should provide sufficient advance warning.
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. The LaneWatch camera system will collect data of alleged contraventions for review. However, the decision as to whether a contravention of parking regulation has occurred is a matter for the CEO reviewing the data to determine.	
4.7	**Data Retention Period - how long will the data be kept?**	
	Data captured by the LaneWatch cameras will be retained for a maximum period of two years. However, in cases where there is ongoing / outstanding legal action, data may be retained for longer period as necessary.	
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.*	
	Dedicated servers on Camden's network infrastructure, which is also managed and maintained by Camden.	

5.2	**Where is the data stored geographically?**
	Within the UK.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Directly through the project: • NSL Services Limited (incumbent parking and moving traffic enforcement contractor to Camden) • London Borough of Camden – Parking Operations • London Borough of Camden – Digital Service • Yunex part of Siemens Mobility UK (provider of the LaneWatch Mk3 camera product and review client software, and who will be responsible for the configuration and testing of the camera, issue resolutions and maintenance) • Tyco Integrated Fire & Security (incumbent CCTV support and maintenance contractor to Camden) when undertaking any routine maintenance or fault fixing of the cameras. • WSP Global (the provider of Taranto parking management software, and their customer support team who will be responsible for any database configuration and the maintain the API). **Indirectly, once a PCN has been generated (external to project):** • Drivers & Vehicle Licensing Agency (DVLA) for the purpose of identifying the 'registered keeper' of the vehicle. • Registered Keeper of the vehicle, as identified by the DVLA, for the purpose of serving a PCN, any appeals or challenges against. • London Tribunals, Environment and Traffic Adjudicators (ETA) and Parking Adjudicators at ETA. • Enforcement Agents working on behalf of Camden – Marston Holdings, Equita and Newlyn.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Access to the servers is restricted and protected to industry standards, with appropriate protection policy in place. Only Camden approved persons will access the servers using the appropriate review client software. CEOs access the data through dedicated workstations, licenses, software key, and the use of RBACs (Camden and Siemens).
5.5	**Is there an ability to audit access to the information?**
	Yes, the servers, cameras, and software systems can generate event logs which can be retrieved on request.
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 captured data does not contain any personal identification information outside of that of the VRM, which on its own cannot be used to identify a living person. For that a separate application to the DVLA would be required to identify the registered keeper and this would need to satisfy their data release criteria. The data servers used by Camden are subject to industry standard protection that aims to prevent unauthorised access, data inception, and similar. Access to the data is through the Metro system and dedicated workstations. These are configured to work in tandem with our network, metro software, licence keys, RBACs and security protocols. Both the Metro system and our network use self-diagnosis and monitoring tools to alert itself to any exceptions and to generate event logs which can be used to audit access.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Yes. This project was initially conceived in 2018 and was subject to full CDS scrutiny. The scope and the outputs of the project was found to be acceptable.

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**
Human error which leads to a data breach; The risk here is that a CEO reviewing the captured data incorrectly records the VRM of the vehicle or that of a cloned vehicle when generating the PCN. If undetected in time this could mean a request is made with the DVLA for the registered keeper details which are unrelated to the event. The consequence would be that a random person who is unrelated to the vehicle or contravention receives correspondence that reveals the whereabouts and actions of	Possible	Negligible	Low

another driver and vehicle at the material time (a minor privacy intrusion). This would also have implications for 'data accuracy' requirements under the DPA. Corporately, this would have some reputational damage attached.			
New impact to privacy; The use of unattended cameras in streets, places, and areas where historically CCTV has not been used before will create new privacy impacts, some which will not be fully understood until after the cameras have become operational. This is more of a concern for places which are by definition sensitive i.e. community health centres, hospitals, places of worship, high commissions, police stations and prisons for example. Compliance: The lack of prior monitoring means some risks will not be identified until after the cameras are operational and Camden will need to be very responsive in terms of mitigation. Corporately: this may generate considerably bad press for Camden and harm its reputation and perceived competence in the eyes of the public.	Likely	Moderate	Medium High
Unauthorised disclosure of footage or images by recipient of PCN; A person who receives a PCN for contravening the traffic measure may, as part of their appeal or challenge, they engage or seek support of third parties to assist. This may mean uploading the video footage by re-recording it using a camera phone, digital camera or similar and uploading it to a file-sharing or video-sharing site, social media or online forum(s). This would mean a number of unrelated persons becoming aware of the matter. Furthermore, it is possible that someone may recognise persons in the video footage or may be able to identify the person through an online witch-hunt. Depending on the circumstances, this could cause the identified person(s) some shame or harm (including self-harm) if it was particularly sensitive i.e. the person visiting a sexual health centre or being escorted in restraints to a police station. The risk is hypothetical, as Camden does not hold any data on the probability of this event occurring and there are a number of considerations which would influence the difficulty of this undertaking i.e. the cameras depth of view, the clarity of any background imagery and digital noise. Compliance: this would wholly be an external non-compliance issue with the Data Protection Act as Camden has put in place a number of protected measures to reduce the risk but cannot realistically prevent a person from re-recording the footage while adhering to the requirements of the parking legislation (showing the footage).	Likely	Minor	Moderate

Corporately: minimum reputational damage for Camden.			

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?
Human error leading to data breach.	**Accept / reduce the risk through mitigation;** The review client software is designed with a number of features to reduce the probability of human errors in the recording of the VRM. These include the need to authenticate the VRM in the footage, duplicate the response, and DVLA vehicle check (make, model, colour, etc of the vehicle). Collectively, this will reduce the likelihood of any VRM errors. Should these measures fail where for example the vehicle is displaying a cloned plate, Camden has processes and procedures in place to purge the system of the data and withdraw the PCN on acknowledgement. Collectively, this would provide mitigation against the risk.	Reduce likelihood and impact	Minor	
New privacy intrusion	**Accept / reduce the risk**; there are several methods available to Camden to raise awareness of traffic schemes and to gain insight into any potential issues with the undertaking. • Undertake on street surveys of the location to understand the use and function of the location. • Ensure traffic restrictions are clearly signed on street through the use of appropriate traffic signage (as covered under the TSRGD) as these will be familiar to motorists across the UK and EU. • Use advance warning signs for schemes where possible.	Reduce likelihood and impact	Minor	

	• Ensure the requirements relating to public consultations are undertaken and suitably broad to cover the nature of the road use. • Ensure the traffic order procedures are followed given persons time to raise any objections or concerns so these can be incorporated into the scheme where reasonable. This process normally takes 6-weeks to complete. In respect to Experimental Traffic Orders, Camden can amend these up to six months from the making. Regular traffic orders will require a different legal approach. • Cameras where surveys show a privacy concern will be brought to the attention of Information Rights Team and their advice sought as to whether the privacy intrusions are acceptable, or mitigations are needed such as privacy masking or adjusting the field of camera vision. **Actions**: Transport Strategy to undertake comprehensive communications with stakeholders / audience to raise awareness of proposals and captured feedback. Ensure all traffic signs are installed in accordance with the TSRGD to avoid any issues for motorists. Use feedback to tailor the delivery of schemes.			
Unauthorised disclosure of footage or images by recipient of PCN.	**Accept the risk**; Camden is limited in what it can do to further restrict access to the footage, as providing it is a legal requirement within the legislation. Camden has already deployed several protective measures to reduce unauthorized access / sharing of data: - All council and contracted employees with access to this data are bound by the council's employment terms and misusing information would be a disciplinary offence and may be a criminal office. - all contracted companies have undergone data protection due diligence which includes assurance	No change in risk	Moderate	

	about employee checks, policies, and data protection training. - The PCN recipient's access to data is through an authentication process whereby a person would need the VRM and the PCN reference to access the data in the first instance. - The video file cannot be downloaded, saved, or sharing of any http link. Once data is accessed by the PCN recipient, the onus on compliance would fall on the person, particularly as to share the data would mean knowingly circumventing the protective measures we have made. In theory, if Camden become aware of any uploads, we could potential submit a 'take down notice' to have it removed if the footage could be deemed protected under intellectual property, copyrighted and similar or where it has been illegally disclosed. However, this hasn't been tested at law yet.			
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**	**No.** **Sarah Laws, Information Rights Team Leader.**
DPO advice	Approved, Andrew Maughan, DPO, 10th March 2022
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	New Draft	March 2022	[redacted]
1.1	Amended risks	March 2022	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?*

-