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.

Project Name	**Camden Mews NW1 / Videalert Trial**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted] Operations Expert
	IAO name and asset	Peter Mardell Head of Parking Operations
	IAO name and asset	N/A
Summary of the project	This DPIA has been submitted as Parking Operations in partnership with Transport Strategy are considering the installation of a new type of unattended traffic enforcement camera into Camden Mews NW1 in response to requests for help from residents. The northern section of Camden Mews sits between Camden Road and York Way and is often used by motorists as a shortcut to avoid queuing traffic around the area. This has meant that residents living on the northern section of Camden Mews are currently subjected to excessive levels of vehicle traffic, noise and pollution throughout the day. Consequently, complaints have been received by Camden over the years about the issue from residents. For context purposes, Transport Strategy undertook a traffic survey of Camden Mews in early 2022 which indicated that around 2,300 vehicles use the road during weekdays. One of the biggest challenges to resolving the problem for residents is the design and layout of the road, which is not supportive of large infrastructure being installed. Indeed, the narrowness of the mews and the need to maintain existing pedestrian access has made finding a suitable solution quite challenging. Prior to arriving at the use of CCTV, Camden has investigated other options, including considering the introduction of barrier gates, and voluntary controls on vehicle access, whereby compliance is foster rather than forced through regulation. However, these options were found to be ineffective to resolve the problem. In turn, Camden is now investigating the use of a new type of camera system, which is based on a modular design concept and able to provide significant coverage of the road to alleviate the issue.	

	Camden believes that it has found a solution in the Videalert unattended CCTV enforcement system and through this project proposes to evaluate the product. **Videalert Product** The Videalert product is designed as an automated, reactive camera tool which only captures data when a vehicle has been identified by the system as having committed a parking or moving traffic contravention. In this setting, the camera product will not capture data unless a contravention occurs and its relative impact to privacy is limited. The camera product has been verified and approved by the Department of Transport for the purpose of traffic enforcement and issuing of Penalty Charge Notices under the Traffic Management Act 2004. Accordingly, Parking believe that the use of this camera product is acceptable for the purposes of reducing vehicle traffic on the northern section of Camden Mews NW1, which it aims to achieve through this project, although on a 12-month trial basis. If a successful outcome is achieved, Camden may consider the use of this camera for similar locations. **Proposed implementation and processing** The Videalert product will be deployed at two points in Camden Mews to provide full camera coverage of the northern section of the road for the purpose of monitoring the 'no motor vehicle' prohibition but also to support the "except for access" exemption. The Videalert product uses a 'master' and 'slave' camera configuration, which means there is main master camera and processing unit and a secondary slave camera that only relays video back to the processor unit. In operation, this allows both video signals to be merged into a single source file by the processor unit and provides significant insight into the movement of the vehicle through the entire zone (the northern section of Camden Mews). The northern section of Camden Mews NW1 is roughly 140m long, while the speed limit is 20mph. Using a speed by distance calculator that means it would take a vehicle around 25-seconds to travel the full length of the road at max speed. Therefore, captured video clips would be between 20 – 30seconds long to capture contraventions. Once the system has identified a contravention, the data will be captured and transmitted wirelessly to a hosted, cloud-based server where it will be stored until reviewed (processed) into a Penalty Charge Notice or rejected and deleted by a Civil Enforcement Officer (CEO). As part of the trial, a camera whitelist may be developed for residents within Camden Mews to enable them to enter and exit the road as necessary. The

	whitelist will be developed on the principle of consent, whereby the residents request to be included on the whitelist. Captured data from the device is accessed via a 'Software as a Service' ("review client") platform. Connections to the platform are regulated by the provider and require authentication. Once a clip has been verified as a contravention by a CEO it will be exported from the review client into Taranto, the council's Parking Management System using a secured API.
Implementation Date:	01/11/2022

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 has been completed and need not be duplicated.

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.

If you have not already done a pre-screen and have been asked to proceed straight to a full DPIA, 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. This is a new type of unattended CCTV camera ("Videalert product") that is of a modular design, meaning two or more cameras can be connected together to enable wide area monitoring and the data ("footage") can be merged into a single video file. For completeness purposes, the Videalert product uses Video Content Analytics in conjunction with Infra-Red (IR) and Automatic Number Plate Recognition (ANPR) to

		detected vehicles, the latter being a technology that is built upon Optical Character Recognition technology from the 1970s.
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	**No.** The cameras will be deployed as part of an existing traffic scheme and will operate against the specified control hours of the measure(s) as set out in the Traffic Management Order and supported on street through appropriate traffic signage (under the Traffic Signs Regulations and General Directions).
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.** The cameras will capture video footage (short clips) of moving traffic contraventions only, which will be reviewed by Civil Enforcement Officers to determine if a Penalty Charge Notice (PCN) should be issued.
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.** This is outside the scope of the project.
1.5	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	**No.** At the point of data capture and during the review process no additional information will be available outside of what can be determined directly from the footage. For example, we will not know who the registered

		keeper is at the time, the history of the vehicle, any persons or property in the captured footage. In this setting, anonymity is not impaired using a Videalert camera.
1.6	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	**No.** The project will be limited to Camden and Marston Holdings: i. **NSL Services** who are the appointed civil parking enforcement contractor to Camden and will supply the labour in form of Civil Enforcement Officers to review any captured data. ii. **Videalert** who will supply the camera product and associated items to Camden for the trial. Which are both subsidiary companies of Marston Holdings.
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	**No.** The Traffic Management Act 2004 and associated statutory instruments set out procedures for the

		issuing of Penalty Charge Notices under these powers, which traffic authorities are legally required to comply with. Personal data will therefore be processed in accordance with those requirements. The Department for Transport has issued Statutory Guidance which explains the procedures, and which can be viewed from the DfT pages here. Captured data will not include any special categories of personal data.
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	**No.** There are no changes to the way Camden is processing personal data for parking and moving traffic contraventions through the Videalert camera product. The existing arrangements will still apply. The Videalert product is purposely designed for traffic enforcement and is limited by design, which renders it unsuitable for public space surveillance.
1.9	Will data be combined, compared or matched from multiple sources?	**No generally.** However, for the purpose of issuing a Penalty Charge Notice under the regulations, it will be necessary to identify the

		"registered keeper" of the motor vehicle who committed the breach of traffic regulations, which is achieved by using the VRM in the captured footage against the DVLA's KADOE system.
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	**No**. The Videalert camera product and CCTV software is unable to process biometric data, and neither can Parking Operations.
1.11	Will the personal data be processed out of the U.K?	**No**. The hosted servers are located within the United Kingdom.
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**. There is technically no minimum age for when a person can legally own a motor vehicle. However, the minimum age for a person to legally drive a motor vehicle on the highway within the UK unsupervised is 17-years of age. Accordingly, this represents the potential minimum age of a recipient of a Penalty Charge Notice.
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	**No**. The activity of the traffic enforcement is covered under primary and secondary legislation, which includes procedures for the processing of personal data in relation to traffic contravention and Penalty Charge Notices. In addition, statutory guidance has

		been issued by the Department of Transport which provides further advice on the use of these powers.
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	**No.** This is outside the scope of civil parking enforcement and this project.
1.15	Will personal data be processed which could result in a risk of physical harm in the event of a security breach?	**No.**
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	**No.** Not through this project or during capture and review processes. Externally and for completeness purposes, while the matter of a PCN is generally a closed matter limited to the registered keeper of the vehicle concerned and Camden, additional parties may be involved in the process where certain conditions are met: i. Where the PCN remains unchallenged and unresolved outside of the appeal stage, and where the local authority engages Enforcement Agents to conclude the matter. ii. Where the registered

		keeper requests a personal hearing with the Parking Adjudicators ETA). Both ETA and Enforcement Agents will be subject to UK data protection requirements.

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/Change		
								There are no changes to the way personal data will be processed for CCTV traffic enforcement through this project. The delivery of the project is limited to a new type of camera only, and one which does not require a human operator to start or end monitoring session, or to capture data. In this sense, the camera product will have a reduced impact to privacy (the change).		
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):*				At the point of capture and during the review process only the vehicle registration number will be known (the personal data) as this can be determined via the captured footage. No additional information will be available to Camden at this time.					
	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):*				**None.** At the point of capture and during the review process only the vehicle registration number will be known from the footage. No additional information is available to Camden at that time.					

		External to this project: Once a PCN has been generated within our parking management system, and the registered keeper details have been furnished by the DVLA, the PCN will be posted to the supplied name and address. In turn, the person receiving the PCN may choose to appeal and through this process voluntarily disclose sensitive personal information in scope of the above items. Possible disclosures have been marked * for reference.
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	**No.** However, it is theoretically possible that a vehicle is driven through Camden Mews without the consent of the owner (stolen) and Camden only becomes aware subsequently once a PCN has been issued to the registered keeper. Furthermore, recorded contravention footage may show things happening in the background that allude to criminal behaviour i.e. anti-social behaviour, violence, drug taking or similar. Parking does not hold any data on the probability of this series of events occurring but imagines that it is generally a low risk.

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data**	In summary: 1. Point of Capture: The camera will identify a contravention using onboard software and will capture the relevant data from both cameras for review (normally a 15-20 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 review client CCTV software ("Event Management Console"). 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 create a Witness Statement entry for the contravention / PCN for audit purposes. 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. Externally from the project: 4. Once data has been received in Taranto and a PCN case created, an automatic process to request the registered keeper's detail will be made with the DVLA through the KADOE framework. 5. The DVLA will provide the registered keeper details where these are known and a PCN will be posted to the name and address supplied. This effectively concludes the processing as part of the project. However, there are additional external steps, but these are not covered.
3.2	**Explain in as much detail as possible why this is being done**	The project aims to support the following Camden objectives: • To help support Camden Plan objectives around sustainability, air quality and local environment as set out in the 'clean, vibrant, sustainable places' ambition. • The use of modular camera technology will support, if successful, the ambitions of the Camden Transport Strategy and

		Air Quality commitments which are centred on tackling climate change and improving air quality in the borough via the delivery of green traffic schemes. • To support Camden in its statutory duty: - To effectively manage our road network under section 16 of the Traffic Management Act 2004 and section 122 of the Road Traffic Act 1988. - To improve road safety by taking reasonable steps to reduce and prevent accidents under section 39 of the Road Traffic Act 1988. - To support Camden's "public sector equality duty" under section 149 of the Equality Act 2010 in relation to advancing opportunities and eliminate barriers for disabled persons to use the highway, in part by taking proactive steps to make the highway more accessible by removing obstacles which hinder use i.e. inconsiderate, dangerous parking or driving by other motorists. • Provide opportunities to improve or develop new Business Continuity Planning (BCP) as the trial may provide Camden with new mitigation strategies to help against any supply chain, quality control, availability, or compliance issues for the CCTV operation. • Support the ambitions set out in the London Mayor's Transport Strategy, including making road safer, reducing injuries and deaths from transport related accidents as part of the Vision Zero Action Plan, Cycle Action Plan and the Walking Action Plan. • Camden has a public health responsibility to the residents of Camden Mews and through this project will address concerns raised regarding the excessive volume of traffic using the

			road, the noise and air pollution caused and the effect this has on their health and wellbeing.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Data captured by the cameras will general not be shared except as stated in responses to question 1.6 and 1.16.
	External organisation or partner Name	**Controller or Processor?**	**Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection? Yes/No/In progress**
	Videalert (part of Marston Holdings)	Processor	**Yes**. Will provide the camera equipment and associated items under agreement. Agreements are already in place with the parent company Marston, but individual agreements will be entered into for data-sharing, confidentiality of information and data protection with Videalert.
	NSL Services (part of Marston Holdings)	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**. An existing contract for the support, maintenance and provision of CCTV cameras and associated equipment, which may include the Videalert product if the trial is successful and arrangement continued, with who we have data-sharing, confidentiality of information, and data protection clauses and sub-agreements.
3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake.**		**Yes.**
3.5	**How will the information be processed/shared. Details eg secure file transfer**		The Videalert camera product will be installed on the highway, usually attached to public realm infrastructure, and will monitor road traffic regulations against a specific configuration. Once an event (a contravention of the restriction) has been identified, the camera system will collect the relevant data, package, encrypted and transmitted it

		wirelessly over 4G or 5G cellular telecommunication network to a hosted (cloud) server. The servers are maintained by Videalert and sit behind industry standard protection i.e. firewalls, port filtering, BRACs, geo-filtering to maintain platform/server security. Incoming data is stored on a server pending review and once completed is archived on a second server in line with our data retention plan. In addition, the hosted servers are supported by appropriate business continuity plans that aim to restore and keep the system operational in the event of server failure or disaster recovery.

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: Processing of data for the project is made under Article 6(1)(e) of the GDPR. Relevant legislation is s.16 and Part 6 of the Traffic Management Act 2004 and s.122 of the Road Traffic Regulation Act 1984.	**Special Category Data:** **N/A**	**Criminal data:** **N/A**
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Tights Team have advised this is appropriate**		
	The convention of consent is not the legal basis for processing personal data under this project. Camden instead relies on the provision of Article 6(1)(e) "task carried out in the public interest". However, in preparation of the whitelist, VRM information will be collected through cooperation whereby a person submits a request to Camden to be included on the exemption list. Without persons providing this		

	information an exemption would not be possible, but is not our legal basis for processing under the DPA 2018.	
4.3	**How will you ensure data quality and data minimisation?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below	
	Data collection is limited to what is required to enable enforcement of traffic regulations only. As such, at the point of capture and during the review process only the VRM will be known directly from the footage and needs maintaining thereafter. Externally from the project: Camden has quality control processes in place to manage VRM data within its systems, including appropriate deletion policy for any errors or cloned VRMs.	
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, as reasonably possible.** It is currently impossible to identify in advance which motor vehicles which will breach traffic regulations and to then provide the registered keeper or driver with a privacy notice at the point of capture. To raise awareness of the traffic cameras appropriate on street CCTV signage will be installed at the location which sets out details for the operator of the camera. In addition, on street signage for the restriction will be installed which gives drivers an opportunity to avoid being filmed. The scope of personal data being processed is covered within the Camden's and Parking Operations Privacy Notice, which can be freely viewed on the council website.
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. A CEO is directly responsible for determining if a breach of traffic regulations have occurred.	
4.7	**Data Retention Period - how long will the data be kept?**	

	The data retention plan is still subject to agreement but would be based on the duration of the 12-months trial.
	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 servers are provided by Videalert and are on the HPE ProLiant platform.
5.2	**Where is the data stored geographically?**
	Within the United Kingdom.
5.3	**What roles will have access to the information?** (list individuals or staff groups)
	The following through the project: • Videalert: who is the manufacturer, supplier of the Videalert camera product and will be providing the servers. Generally, this will be limited to their technical support team who will be responsible for the installation, configuration of the cameras, the management and resolution of issues, and maintaining the camera product thereafter post-trial. • NSL Services Ltd: through CEOs who will be responsible for processing captured data from the cameras. • Parking Operations (Operations Team and Process) who are responsible for any PCNs that are issued, but the CCTV team who oversee the operation of the cameras and will be involved in the configuration and UAT processes for new cameras. • WSP: the provider of Taranto parking management software, and their customer support team who will be responsible for any database configuration and the API. • Tyco: who are the awarded Camden CCTV contractor and who will be responsible for the maintaining the cameras and support systems outside of the warranty period. Externally • The registered keeper of the motor vehicle at the time of the contravention. • Environment and Traffic Adjudicators and Parking Adjudicators: where a PCN has been challenged but Camden does not accept the grounds for appeal and hearing is scheduled to resolve the case. • Enforcement Agents (various): if the PCN case remains unchallenged and unresolved.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**

	Physical security at the datacenter is to industry standards. The Event Management Console (EMC) system uses several security features to limit access to the system and data contained within, including geographical blocking, IP filtering, Role-Based-Access Credentials (RBACs), encryption keys and firewalls. Please see 5.3 for details of who can access the data.
5.5	**Is there an ability to audit access to the information?**
	The system generates system logs which can be retrieved and viewed.
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 only data captured by the cameras will be short video clips of motor vehicles and VRMs. On its won a VRM will not contain personal data but could be used in conjunction with other data sources to potential identify a living person. The following measures are in place: - The only data captured by the cameras is short video clips of - Physical measures at the datacenter to industry standards. - Each system deployment is specific to the customer and the data held within these deployments. The servers are presented in an isolated stack and are managed using Group Policy Object specifics to each customer. - Launching the remote desktop and accessing EMC required primary and secondary Role-Based-Access-Credentials (RBACs). - To access data through the EMC will require the presentation of an encryption key which decrypts the video files that are imported to the review client.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Yes. This project was initially conceived in 2020 and was subject to full CDS scrutiny. The scope and the outputs of the project was found to be acceptable at the time, as the product would be run externally to the Camden network.

Step 6: Identify and Assess Risks			
New impact to privacy. The Videalert camera will be through their presence create new impacts to privacy for residents on Camden Mews, as this road has not previously been subject to camera enforcement. There is some ambiguity around what manner of issues will materialise in terms of privacy and our mitigations against, which will only be identified over time. Some fine-tuning of the camera's field of view will be necessary to adhere to privacy regulations. If not properly managed, we could infringe requirements and be subject to legal proceedings if challenged.	Possible	Minor	Moderate risk
Privacy intrusion from cameras taking footage of private property. This would in essence be an infringement of 'Article 8 – Right to respect for private and family life' of the Human Rights Act 1998 and would occur where the camera's field of view peers directly into private property in the context of windows, doors or private gardens. Such images would be seen by Civil Enforcement Officers reviewing the footage and by the PCN recipient seeing the contravention images and footage. Consequences of Camden committing such breaches could result in legal proceedings against the council.	Almost certain	Moderate	High risk
Human error regarding the VRM. This risk would materialise where a CEO having reviewed the captured footage inadvertently enters the wrong VRM or that of a cloned vehicle when generating the PCN. If not detected in time, this could result in a PCN being sent to the wrong person, thus informing them where the driver of the car in question was at any one point (a minor privacy intrusion) and could result in a request to the DVLA for registered keeper details not related to the vehicle in the footage, which would result in correspondence to the keeper in respect of the actions of another driver which would be minimally privacy intrusive. These would also contravene the data accuracy requirements.	Possible	Negligible	Low risk
A personal data breach or breaches. Article 4, item 12 of the UK GDPR provides a definition of a 'personal data breach' as an event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or personal data, including that which is transmitted (intercepted), stored or otherwise processed. This is a wide spectrum of activities but in the context of Camden would likely occur when a VRM is incorrectly recorded, and a subsequent request is made to the DVLA for the registered keepers' details. This would allow for an unrelated party to the matter to gain	Possible	Minor	Medium risk

insight into another vehicle and potentially, behaviour of the registered keeper. In this case, this could amount to a personal data breach, but would be a minor intrusion as no identification of the person would be possible through the images or footage by a reviewer.			

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.

Decide if this is accepted in the 'measure approved?' column. Table 4 provides guidance.

Note that risks and scores are subject to review and change by IRT/DPO

Risk identified in step 6	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
New impact to privacy.	Reduce the risk through a number or mitigation strategies: i. The traffic signs used will be familiar to UK and EU motorists, which means drivers should understand that vehicles are not permitted into this section of Camden Mews. ii. Transport Strategy have been in dialog with residents of Camden Mews and feedback used to tailor the scheme. iii. Public notices may be used to provide advance warning to residents, businesses and emergency services of the scheme going live. Although the restriction has been in place for over 12-months now.	Reduce likelihood and impact.	Minor	yes

	iv. Undertake site surveys to understand what the key issues will be for the camera and privacy. Using this develop appropriate mitigations to limit the impact. v. Review test footage early to ensure compliance with regulations and amend as necessary the camera view. vi. Trial the cameras to develop an understanding of the impact, the risks, issues, and challenges of using these at the location. vii. Respond to any changes in risks accordingly during the trial and use this information when considering a permanent solution to better mitigate impact to privacy. Change or amend the camera view. viii. Review the need for a camera, if the scheme does not see an improvement in compliance perhaps other options will be more effective i.e. physical measures. Collectively, these measures should mitigate the overall impact to privacy.			
Privacy intrusion from cameras taking footage of private property.	The following measures are in place to ensure compliance with privacy and data protection requirements: i. Camden staff understand the implications of the Human Rights Act and Data Protection Act on privacy and take appropriate approach to ensuring this is included in the planning of any camera installations. ii. Camden staff actively seek advice from colleagues in the DPA team for any contentious locations, which is then feedback into the implementation. iii. Amend or change the camera view as necessary or implement privacy masking.	Accept the risk, Reduce the risk and impact,	Minor	yes

	iv. Clear understanding of Camden requirements is known by the Supplier having worked with Camden for a number of years now and a develop approach has been agreed which flags up potential issues in advance i.e. that the camera peers into private property. v. Footage from the cameras is reviewed regular to understand if any of the risks have changed, increased or decrease, where for example a property changes from resident to commercial or commercial to residential and what impact, if any, this has on the camera's field of view. vi. Processes are in place to withdraw any PCNs which have been issued against protocol at the review stage. This approach should help to mitigate the impact to privacy.			
Human error regarding the VRM	Reduce the risk and impact through the following mitigations: i. The EMC software has built in features which require the VRM in the footage to be authenticated, which should identify any issues at the first instant. ii. There is an established process for purging incorrect VRM data from our systems which would be engaged once the mistake has been identified and the PCN withdrawn. iii. CEOs output is monitored for accuracy and issues identified feedback to officers to prevent reoccurrence. iv. Camden regularly reviews output and develops new processes as needed to improve performance i.e. additional training, new software tools, etc. Collectively, we believe these measures help to mitigate the risk posed.	Reduce likelihood and impact	Negligible	Yes

3. Privacy Intrusion from cameras taking footage in nearby properties.	Reduce risk: Officers responsible for the implementation of CCTV cameras have been trained in how to identify and reduce privacy intrusions. The general approach by Officers is to position the camera and field of view in such a manner where it will avoid privacy intrusions in the first instance. Where it cannot be avoided privacy masking will be applied to the relevant area(s) of the camera view. Where there are concerns, there is an established process whereby the highways officers engage with the Information Rights Team to consider trial positional photographs from the cameras to discuss privacy intrusion on a case-by-case basis. Agreements are made about the acceptability of positioning of cameras, posts, angles and sweep before they are installed. In most cases using an unattended camera has a reduced impact on privacy, simply because you cannot operate the camera and the view is static (fixed in place).	Reduce likelihood and impact	Minor	Yes
A personal data breach or breaches	The following measures are in place: I. The CCTV control room is a restricted area where access is not permitted outside of authorised personal. II. All staff are trained in data protection and privacy requirements under the UK GDPR, DPA and HRA. Clear guidance on the use of the camera system and data has been provided to staff which sets out a baseline behaviour expected by Camden. III. Current rules, procedures and prohibitions prevent any electronic or physical copying of data and the workstations do not support exporting outside of the API interface into the Parking Management System.	Reduce likelihood	Medium	yes

	IV. Data is stored on a dedicated server, in an archival system, which is subject to disaster recovery and server recovery procedures which aims to ensure the availability of data. V. Data retention is undertaken in accordance with an agreed schedule and processed automatically by the server based on date values. The full extent of these changes should prevent any data breaches.			
Residual (remaining) risk level when all mitigations have been applied: ***Note IRT/DPO may change this***				
Medium				

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	Andrew Maughan
Information Asset Owner acceptance of residual risks	Peter Mardell, Head of Parking Services
This DPIA will kept under review by:	[redacted], Operations Expert

Version Control

Version	Reason	Date	Author(s)
1.0	**New draft**	**June 2021**	**Tony Crawford, with feedback from Sarah Laws**

1.1	**New draft + amendments**	**June 2022**	**Tony Crawford**

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?*

-