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	Body Worn Cameras for Civil Enforcement Officers	
Project Lead and Information Asset Owner/s	Project Lead	[redacted], Operations Officer
	IAO name and asset	Peter Mardell, Head of Parking Operations
	IAO name and asset	
Summary of the project	This DPIA has been submitted as Parking Operations is seeking to mobilise the use of Body-Worn Cameras (BWC) as part of its civil parking enforcement operation. The BWC devices will be provided and maintained by the civil parking enforcement contractor to Camden, Marston Holdings via their subsidiary company NSL Services Ltd who provide the Civil Enforcement Officers (CEOs) on the contract. The product to be deployed is a Edesix VB400 Body-Worn Camera manufactured and sold by Motorola Solutions. Although the devices are supplied and asset managed by Marston, as their use forms part of the existing contract between parties for services, Camden is considered a 'joint data controller' as per Article 26 of the UK GDPR and Data Protection Act 2018, respectively. The VB400 product measures 7cm x 7cm x 2.5cm and is capable of recording audio and video to H.264 and H.265 standards. The device attaches to the uniform at the chest, facing outwards, and provides a perspective view of what the CEO is seeing and hearing at the time of the recording (the "activation"), including their interaction with the environment, any persons or property within and anything else which happens within the field of view. The VB400 product is fitted with a wide-angle lens which enables it to record 20degrees horizontal, 65degrees vertical and 140degrees diagonal and directional dual microphone. Given this, it is possible that additional information may be captured in the recording that is unrelated to the matter,	

	but which now forms part of the evidence of the event. For example, this may include persons going about their business or having personal conversations in earshot of the device on the highway. Therefore, there is a risk around the operation of these devices, the data collected and the impact to privacy caused. Marston advise in their DPIA that the use of BWC is being undertaken to support the safety and accountability of their Civil Enforcement Officers (CEOs) on street due to the potential risk of abusive, threatening, or violent behaviour directed at them while undertaking duties. It is acknowledged that BWCs do not in themselves provide any physical protection against assault, but their presence acts as an effective deterrent to counter aggressive behaviour in the first instance. This is because these devices produce a factual record of the event that cannot be disputed and which in turn can be used as evidence for police reporting or to support civil prosecution of any culprit(s). In terms of Health and Safety, all employers in England and Wales have a statutory duty of care to protect their employees under The Health and Safety at Work etc. Act 1974, which means taking reasonable steps to protect staff from injury, which BWC will support. **Proposed implementation** There are currently around 120 CEOs deploying each day over a 24-hour period, and who would all under this proposal require a BWC device. The VB400 devices will be deployed and managed by Camden's incumbent enforcement contractor NSL Services Ltd, with Camden not having access to the data except under reasonable causes, such as when investigating complaints or counter allegations against CEOs which shall be managed through a data release procedure. Marston have indicated that upon reviewing any recorded footage, if they believe the conduct of the CEO to be unacceptable or not to have met expectations, they will use the footage for feedback purposes and to offer additional support or training where appropriate. Reviews will also help shape and develop conflict resolution/management strategies and training. ***** UPDATE MAY 2023 *****

	Parking Operations has successfully been using the VB400 device for the past six months and has provided some feedback on its deployment. • Marston has managed to successfully deploy 87 of 123 of the VB400 devices. Unfortunately, we encountered some network connectivity with one of our bases which has delayed deployment until later this year. • Since the introduction of BWCs into the borough there has been a significant decrease in instances involving violence, abusive and threatening behaviour towards Civil Enforcement Officers (CEOs). Prior to the deployment, in the year beginning 2022 up to July, CEOs had experienced six code red and two code yellow incidents. However, following the roll-out in October 2022 we have only had one code yellow occurrence, which was defused by the presence of the BWC and threat of activation. • To date, all the cameras are functioning correctly, none have been reported as stolen or lost. We have also not had any data captured outside of the scope agreed. • The general reception by CEOs has been overwhelmingly positive, with officers noting the presence of the device has resulted in a reduce in aggression towards them by the public. Parking Operations will continue to keep under review the use of these devices and will commit to undertaking a bi-annual assessments of the use of this technology for parking enforcement purposes.
Implementation date	October 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?)	**Yes.** BWC product will be a new technology in relation to the civil parking enforcement contract, but not in the context of Camden who already make use of such devices for other purposes. The product allows for the recording of audio and video footage.
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	**No**. BWCs are a reactive tool and will only be used in a limited capacity in relation to aggressive, threatening, or violent behaviour directed towards CEOs whilst on duty. For context purposes, there were 98 incidents involving violence and 14 reported incidents of abusive and threatening behaviour towards civil enforcement officers in Camden between 2016 and 2021. Averaging around 22.4 incidents per year. A verbal warning will be issued prior to the activation of the device which should mean the overall level of activations is reduced over the life of the contract.
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 VB400 device is manually operated by the CEO and any decision on activation will be taken by the officer based on the situation and in line with any training they received.
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.** BWCs will not create new identifiers. However recorded footage may inadvertently capture identifiers if these are on display, shown, cited, or divulged during the recording.

1.5	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	**No.**
1.6	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	**Yes.** The following: Marston Holdings (NSL Services parent company): who are providing the BWCs and related infrastructure to support the technology, but who also provide the CEO workforce as part of the parking contract. Marston and NSL Services are registered with the ICO: • Marston Holdings Ltd. - ZA054553 • Marston Group Ltd. - Z9930012 • NSL Services Ltd. - Z9798193
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.** The BWCs will create a new stream of data (video and audio recordings) that is predominately related to Camden's function as a 'traffic authority'. This data may or may not contain personal data as per the definition provided in Article 4 of the UK GDPR, but in either case will be processed externally from Camden. Camden will have access to the data for legitimate purposes. Data will be processed for the purpose of reporting crime and prosecution, which is a new purpose in relation to Parking Operations.
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 for Camden as the existing processes of requesting statements and evidence from CEOs in relations to incidents is maintained. However, this project does create a new type of data processing that will potentially contain personal data but may also include criminal behaviour.

1.9	Will data be combined, compared, or matched from multiple sources?	**No**. Generally, BWC data will not be cross-referenced, combined, or matched with other data sources. However, data will be passed to the Police who through their own enquires and powers may do so. It may also be possible to privately identify person(s) using information sourced directly from the footage i.e. the person divulges it. Furthermore, a reference to BWC data having been captured may be recorded as part of the CEO notes assigned to the Penalty Charge Notice. However, the data itself will be treated separately to the PCN.
1.10	Will you process biometric (fingerprint /facial recognition) or genetic data?	**No**. The VB400 product and associated software is unable to process biometric, fingerprint, iris, facial recognition, or hand geometry data.
1.11	Will the personal data be processed out of the U.K?	**No**. The servers are located within the UK.
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**. Data will only be collected by the CEO where they feel there is a risk to their personal safety, in relation to an abusive, threatening, or violent incident.
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	**No**.
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	**No.**
1.15	Will personal data be processed which could result in a risk of physical harm in the event of a security breach?	**No.**
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not	**No**. The parties involved in the scope of BWCs are based within the UK and will be subject to the regulations set

	subject to comparable privacy regulation?	out in the UK GDPR and Data Protection Act 2018. A person(s) involved in any incident may not live in the UK (domiciled elsewhere) and could reside in a country where data protection regulations are not equivalent. However, under UK law a person (the defendant) has a legal right to disclosure of evidence against them, which inevitably means sharing data with the person through legal representation normally.

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 use**. Parking Operations has not previously used BWCs, and the data created will be new for the service. However, in the context of Camden, such devices are already used for personal safety, collecting evidence, security and Health and Safety purposes.
2.2	**What data will be processed/shared/viewed?**	
	Personal Data	
	Other data *(Please state):*	The recorded BWC footage will consist of both audio and video of a person(s) in an abusive, threatening, aggressive, or violent state. Additionally, during the confrontation a person(s) could reveal additional personal information such as: - My name's.... - That's my car... - I live at... - Get your supervisor to call me now on... - I didn't vote [name of political party] for this...

	Clearly, there is a margin of falsehood that may materialise through these statements, which will not be known until or if the information is followed-up.
Special Categories of Personal Data	
The VB400 device records both audio and video to high standard, as such it is possible that information may be sourced directly from the recorded footage either by: • Visual recognition of items, clothing, jewellery, medical aids, or equipment as seen on the person; or • Where the person volunteers such information through dialogue. This may mean identifying the person(s) through their work attire, ID cards, company vehicle or gaining an understanding of their political views, affiliations to organisations, religious beliefs, health conditions or similar. It is equally possible, that the same may apply to persons in the background or passes-by captured in the recording, including persons off camera having conversations. At the point of capture and during review these would be generalisation based on prompts and is not necessarily factually correct. The additional information is also unlikely to be fact-checked.	
Other data *(Please state):*	As far as reasonably possible, the following: **Visual prompts** i. Name of person(s) as stated on any displayed work ID, label, tag or embroidered onto any workwear. ii. Name of current employer as displayed on any work wear, equipment, consumable, or vehicle. iii. Political affiliation, membership of any organisations, religious beliefs, or ideology through the wearing of any pin badges, patches, religious icons, jewellery, merchandised, hats, caps, scarfs and/or tattoos.

		iv. Health conditions through their physical appearance or the use of walking aids, hearing aids, medical devices, asthma pumps or the use or presence of medication, or a disabled blue badge. **Verbal prompts:** i. If the person(s) makes any statements or is overheard during the recording. These statements could in theory cover any number of things, may be unrelated, contain personal information, abhorrent, hateful, harassing, discriminatory, xenophobic, or similar in nature. This also applies to persons in the background.
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	**Yes**. The recorded footage will show the acts of abusive, threatening, aggressive or violent behaviour from a person(s) directed against the CEO. The footage may also show the Police attending, cautioning, or arresting the person(s) and potentially restraining and escorting the person away from the scene. Collectively, this would allude to criminal behaviour but not necessary a criminal conviction as case may be dropped by the Police, Crown Prosecution Service (CPS) or Marston respectively.

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data**	The BWC will only capture data when the activation button has been pressed. This sends out an audible sound and visual indicator that recording is in operation. Prior to activation the CEO will issue a verbal warning advising the person(s) that the device is about to record. In theory, this will give the person(s) an opportunity to disengage from hostility and prevent a recording being made. All VB400 devices will be clearly labelled with 'WARNING audio and video recording' to make these devices more conspicuous to the public. The device also has a physical and audible alert. A Standard Operating Procedure (SOP) will be developed by Marston for the devices that will be incorporated into staff training that will further ensure the devices are used appropriately and controlled. **Processing of data:** 1. Marston will be responsible for the supply, configuration and setting up of associated infrastructure and testing for the VB400 at each deployment base in Camden. The devices will be stored in a secure area of the building and keep on a port dock ready for use. 2. Each CEO who is deploying on street will be assigned a BWC device by a supervisor at the start of their shift. Details of the deployment will be recorded in a daily log. 3. Once a BWC has been assigned to the CEO, the officer will be

		responsible for the device, its use, operation and safe return to base at the end of their shift. Supervisors will undertake reconcile of devices against deployments daily. 4. BWC devices which are unaccounted for, being either lost, misplaced, or stolen will be the responsibility of base managers and supervisors to investigate, locate and retrieve or report to the Police. If a device cannot be recovered for whatever reason a deactivation protocol will be initiated. **In operation:** 5. The VB400 product has a pre-record function where it continuously records the last 30- to 60-seconds of activity before manually being activated. This allows for some context to the recorded footage to be possible and will confirm if a verbal warning was given. If a manual recording is not activated the data is irreversible recorded over. 6. When a CEO activates the record function on the device, the footage is saved locally on the device in the form of a video file and encrypted. While in carriage the data cannot be reviewed or played-back, consequentially data cannot be shared on street. 7. The data which has been recorded at the scene will be stored on the device until it has been docked back at base and a transfer routine activated. The

		transfer routine will extract the encrypted data from the VB400 and transmit this using the Marston Group Private Wan to a secure, cloud-hosted server where it will be stored. Once completed the recorded data on the BWC storage will be purged from the device. 8. In order to view the recorded video file, the relevant installation of VideoManager software will be required that contains the appropriate unique decryption key. 9. Access to the recorded footage will be strictly managed, with only a limited group of persons having access. Any time data is viewed through VideoManager an event log is created. Data may be accessed for several reasons: a. When auditing BWC data against data policy (Marston). b. When collecting evidence to support the making of a police report or to bring a private prosecution (Marston). c. When investigating a complaint, allegation or counterclaim made against the CEO (Camden and Marston). d. When responding to a formal request from the Police for evidence of an incident under their investigatory powers or as part of legal proceedings (Marston).

		e. When processing a request from a person in the footage as part of a Subject Access Request (SAR) (Camden and Marston). f. When compliance monitoring and auditing of recorded data to ensure these accords with policy (Marston). 10. Data is stored on the server in accordance with Marston's Data Retention Plan and schedule, which is currently 45-days from date of data transfer. This is except where there is on-going legal proceedings where the data may be held until the matter is completed. Once no longer required archived data will be purged. **Optional:** 11. The VB400 and VideoManager software include a number of optional extras that can be implemented at any time. These include: a. The ability to livestream footage from the device using a network connection to a control room using the VideoManager software. b. Peer-assisted recording which allows for additional VB400 units to record based on the devices' proximity to the original device that has been activated. This is quoted as a distance between 2m and 10m and is configurable. Data can then be collected from multi-

		devices and compiled using the VideoManager software. These features are persistent within the software and devices meaning they can be enabled at any time through an update to the global device setting/configuration. At the time of writing these functions are disabled and will not be implemented, having been provided for completeness purposes only. An update to the DPIA will be submitted if that situation should change in the future.
3.2	**Explain in as much detail as possible why this is being done**	The project is being implemented for the purpose of meeting the 'duty of care' requirement set out in section 2 of the Health and Safety at Work Act, etc. 1974 which requires employers (in this case Marston and NSL Services) to undertake a range of measures to protect their employees from injury. The physical presence of the BWC should act as a strong deterrent against any verbal abuse of physical violence. For context purposes, between 2016 and 2022 there were 112 incidents reported by CEOs, of which 98 involved violence. The recorded footage from the BWC will provide a factual, indisputable evidence of the incident which can be used to: - Make a Police report for the purpose of bring charges against any person(s) involved; or - Bring a private prosecution against any person(s) under section 6(1) of the Prosecution of Offences Act 1985). **Benefits** • To support CEOs in undertaking duty without the fear of violence or abuse by members

		of the public. • To support the reporting of crime to the police and avoid the interpretation of events through the production of a factual, undisputable record of the incident. • To enable legal recourse, private prosecution or legal remedy / restitution against any persons that have acted violently towards CEOs. • To help develop mitigation strategies to de-escalate aggressive situations.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**	**Yes.** Marston will be responsible for disclosing any information to individuals or organisation as they will be holding the data on their network. Camden will be involved in approving releases, as a joint data controller. Parties for release: I. The Metropolitan Police in respect to making a Police report and supporting criminal proceedings. II. Living persons under an SAR application made for the recording. III. Any other third parties such as UK Courts and Environment Traffic Adjudicators. IV. Health and Safety Executive for any workplace or work-related accidents or near misses under the RIDDOR reporting regulations as captured in the recording.

	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**
	Marston Holdings Ltd	Joint Controller with Camden (Parking Operations)	**Yes**. There is an existing contract between parties for civil parking enforcement and related services, which includes provisions relating to data protections, confidentiality, data-sharing and suitable sub-agreements.
	Has a data flow mapping exercise been undertaken? **If yes, please provide a copy, if no, please undertake**	**Yes.**	
3.4	**How will the information be processed/shared. Details e.g., secure file transfer**	Information will be processed in the following manner. - CEOs on street will activate the BWC to capture data initially. The data will be stored locally until the BWC is docked. Data will be transmitted via Marstons WAN to a dedicated, secured, server where it will remain in line with the 'retention policy'. - Marston uses a private multi-protocol label switching (MPLS) based network which is a traffic routing mechanism within telecom networks to connect to their infrastructure. It allows each customer's data to be kept separate from other data	

		streams using specific labels that direct data along pre-determined paths through the network. - The MPLS is a private network and traffic routing service that creates private lines by directing data based on predetermined labelled paths within the network. - Server data is restricted and will only be available to specific persons using VideoManager: • The data is available to members of the Audit and Legal Teams within secure Group locations. • Additionally, named authorised manager/s on individual contracts will have availability to view BWV/Audio. Viewing is strictly controlled and recorded. From time to time, access is permitted to additional personnel and/or clients for the purpose of investigating complaints, incidents, evidencing that visits have taken place at specific properties and to respond to legal proceedings. Approval to release data will only be made by the Audit and Investigations Director. Information will be shared using the following approach:

		• Data sharing will only be possible once a formal request is received. • Requests for data will be reviewed in line with Marston's data release policy. • Video files will be shared either physically or electronically and will be protected to prevent unauthorised access. • Access credentials or encryption key will be shared separately to the video file to prevent unauthorised access. • A record of data having been shared will be completed for each release. • If Marston is contacting the police about an incident, the video file may be included as part of the submission or provided afterwards. This approach will be reviewed regularly to ensure it is compliant of data protection regulations.
3.5	**How will the data be stored?**	Data is collected in Camden and transmitted to a secured server(s) within the UK. The servers are provided on the Azure cloud service platform and are compliant of ISO/IEC 27001:2013 security standard and NCSC certified for Cyber Essential Plus amongst other things. All data on the server is encrypted requiring an appropriate decrypt key and relevant VideoManager installation. Access to the data is controlled by a reasonable causes policy which aims to limit access except where necessary. Marston have introduced an internal process for this, which uses their audit and legal team to determine if access is warranted i.e. Police requests, SARs,

		and complaint investigations for the data collected. In this configuration. Camden would only have limited access to the data, having first to satisfy that a release is required. The Azure platform provides appropriate level of server resilience and disaster recovery options to subscribers in critical failure scenarios to recover data.

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**
	The following: • Personal data: Processing of personal data is made possible under Article 6(1)(e) ("public task") of the UK GDPR which recognises the role of Camden as a 'Traffic Authority' and its functions under the Traffic Management Act 2004, Transport Act 2000, and Road Traffic Regulation Act 1984. • Employers "duty of care" for their staff as set out in section 2 of the Health and Safety at Work Etc. Act 1974 as covered under Article 6(1)(f) ("legitimate interest") of the UK GDPR - Marston. • To report any criminal offences, undertake civil proceedings or legal remedies or resolutions under Article 6(1)(c) ("legal obligation") of the UK GDPR. • Special Category of data: Article 9(g) reasons of substantial public interest (with a basis in law) under The Data Protection Act 2018, Part 2, Schedule 1 Conditions and Paragraph 6 Statutory and Governmental purposes, Paragraph 10 Preventing or Detecting Unlawful Acts. • Criminal Offence Data: Article 10 of the UK GDPR is met by Article 6 and Schedule 1 of the Data Protection Act 2018, Paragraph 6 and Paragraph 10 as above.
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 for processing personal data under this project. That being said, CEO will be required to verbally advise the BWC is going to record which will allow for any hostility to be disengaged, thus preventing a recording being made. If the person(s) continues to be aggressive their action(s) can be taken as a form of implied acceptance. Where the CEO is ambushed or attacked without warning, it may not be possible to give a verbal warning.	
4.3	**How will you ensure data quality and data minimisation?** To achieve the evidence standards required to bring a case to Court, evidence must either be beyond 'reasonable doubt' in criminal cases or the balance of probability in civil cases. Inevitably, in either scenario the BWC footage will be principal to proving the case against any defendant. The VB400 device is purposely designed and built using modern day parts and components that met the requirements of capturing audio and video to a high standard. The device is currently used by several local authorities, police forces, HM prisons and emergency services, which highlights its suitability. In terms of data 'data quality' this is achieved with modern camera lens and microphone technology which collectively produce a clear, undisputable record of the event as a video file. Data minimisation will be achieved as data is only captured after a verbal warning has been issued and where a manual activation has been triggered in response to aggressive behaviour directed towards the CEO. Data captured will predominately show an act(s) of threatening or violent behaviour and would be captured in the 'public interest' for the purpose of criminal justice, which is an appropriate outcome, not being excessive or disproportionate to that purpose. Data will be retained in its raw state for 45-days generally but may be held longer depending on the course of any legal proceedings. However, once the data is no longer required it will be purged from the Marston server.	
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 far as reasonable possible.** The BWC devices will be clearly labelled with audio and video recording, which should provide a clear visual warning. In addition, CEOs are required to verbally inform person(s) that the device is about to be activated for making a police report. Collectively, this will provide persons with advance notice of the processing and an opportunity to avoid being filmed.

		Parking Operations have updated our Privacy Notice to refer to the use of BWCs.
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. Camden does not hold the data but will instruct Marston to release if requested. Alternatively, Marston will be responsible for complying with a DSAR request in the same manner as Camden. There are appropriate clauses within the contract between parties to facilitate these requests and for such purposes.	
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?**	
	Marston's Data Retention Plan currently permits for data to be held for 45-days from transfer. However, it is acknowledged that there may be occasions where data must be held longer for where legal proceedings are taking longer than expected. In such cases, the data will be held until the matter is completed.	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*
	Data from the BWCs will be held on servers on the Azure platform which is compliant of industry standards and data protection requirements.
5.2	**Where is the data stored geographically?**
	The servers are located within the UK.
5.3	**What roles will have access to the information?** (list individuals or staff groups)

	The following **Directly through the project:** • NSL Services Ltd (part of Marston Group Ltd) the incumbent parking and moving traffic enforcement contractor to Camden. • Marston Holdings Ltd – Audit and legal teams for the purpose of investigating complaints, incidents and to respond to legal proceedings. Approval to release data will only be made by the Audit and Investigations Director. • London Borough of Camden – Parking Operations, Central Complaints, legal Services (if the matter relates to a Court case) and Internal Audit. **Indirectly (external) to the project:** • London Tribunals, Environment and Traffic Adjudicators (ETA) and Parking Adjudicators at ETA, if the evidence requested. • Police in relation to threatening or violent behaviour direct towards CEOs. • Courts, Judiciary, and legal representation (lawyers, legal advocates, and barristers) for prosecution purposes. • Health and Safety Executive (HSE) under the RIDDOR regulations.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Yes. Access to the servers is restricted and protected to industry standards, with appropriate protection policy in place. Only approved persons will access the servers and data stored within. Please see response to 5.3 for details of who can access the server data.
5.5	**Is there an ability to audit access to the information?**
	Yes. Please see response to question 5.3 previously.
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 following: • BWC devices do not permit any viewing of captured data on street and must be docked to upload data before it is available to view. • Marston use their own private WAN for transmission of data to the Azure platform. This is a restricted network, which has appropriate monitoring and protection in place.

	• BWC devices are purged of data once docked and there is no means to retrieve the data from the devices. • Access to the data is restricted on the Azure platform; using appropriate software, licence key(s) and RBAC specific persons at Marston's can access the data. • Access to the data is managed through internal procedure (reasonable cause) and this is overseen by Marston's audit and legal teams to ensure legal compliance with the Data Protection Act 2018 and UK GDPR. Camden does not have any direct access rights by default to the data but may request it for investigation purposes. • Access of the data is monitored and recorded in event logs, which can be retrieved from the system for audit purposes. • Data is held temporarily for a period of 45-days (data retention policy) after which time the data is purged from the server unless archived data is required for ongoing legal proceeding. • A person wishing to exercise their statutory data rights (SAR) may do so. However, due to the temporary nature of the recorded footage, this would need to be requested within a reasonable time of the event taking place, within 45-days as the data may be purged after this time.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Yes. There were no security concerns as the technology bypasses Camden's IT environment.

Step 6: Identify and Assess Risks			
Describe source of 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)** Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA* *Note that risks and scores are subject to review and change by IRT/DPO*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Inherent privacy intrusion where the BWV records a person without consent including audio. The risk occurs because persons may be seen or heard in	Possible	Negligible	Minor

the background while the BWC is recording. Consequence: Under UK law, evidence in court cases must be relevant and admissible, it must prove the offence to which the defendant is charged. This means that the BWC recording is primary evidence to substantiating the charges against the defendant. Furthermore, evidence cannot be tempered with (edited, reframed or similar) as to do so could result in it being inadmissible. Collectively, this means evidence must be preserved in its entirety as it was collected at the scene. It will likely be played in Court to substantiate any charges or claims and may be subject to challenge or even expert review. Altogether, this means it likely that any captured evidence will be shown in Court. This would amount potentially to a privacy intrusion for any background persons, who through the recording will loss control over the use of their data, possible shame, embarrassment or even stress if the evidence is presented at court. Compliance: BWCs will operate on a reactive basis, in response to verbal abuse or physical assault. In this setting, it is an appropriate outcome and accords with the intention of data rights not to restrict the good function of society and other legal responsibilities, rights, etc. For context purposes, in the past five years we have seen on average 22 incidents per year which suggests the devices will be used sparingly.			
Unauthorised release of data. The risk would materialise where captured data relating to an incident is leaked to the public by a person who has access. Consequences: depending on what is captured in the footage and the manner in which the data is shared, it could mean the person(s) in the recording are identified through visual recognition or by an online witch-hunt for the purpose of naming and shaming or similar. Depending on the incident, the person(s) in the recording may face some public backlash.	Rare	Minor	Low

Compliance: in this setting, the release of data would be authorised, conflicts with the protective measures in place, data protection regulations. It would be a wanton act potentially designed to shame the persons and obtain some justice for the victim. This is something that Camden would not condone, but given we are a joint data controller there could be some reputational damage at stake if this should materialise. It is likely to be an offense under section 170 of the Data Protection Act 2018.			
Failure to advise person of BWC activation. This would occur where the CEO either fails or is prevented from giving the verbal warning i.e. is ambushed or attacked without warning. Consequences: failure to give a verbal warning could be a missed opportunity to take hold of the situation and de-escalate. It would also potentially deny any persons an opportunity to avoid being filmed. Compliance: The Data Protection Act 2018 and UK GDPR require reasonable steps be taken to give persons advance warning of the processing of their personal data. Accordingly, CEOs are required to verbally advise that the camera is about to activated. However, there may be situations where this cannot reasonably be done, where the CEO is subject to spontaneous, unprovoked aggression or violence. English law does not take a position on the rights of persons to privacy in the public space. Accordingly, an individual cannot reasonably hold an expectation of privacy when going about their business on the highway, and more so when involved in a verbal abuse, aggression, or violence against another person in a public place. In this setting missing a verbal warning could be unfortunate but would not significantly change the impact to privacy, particularly as the VB400 device is labelled with 'WARNING audio and video recording' and has physical indicators and an audible alert when recording.	Unlikely	Negligible	Low

Recording without consent or lawful basis. This risk would materialise when a CEO for whatever reason activates the record function outside of the agreed policy and with or without warning. There could be a number of reasons for this, good and bad intentions, in a public or private setting, covertly or overtly in nature. However, as potentially personal data is being recorded this could be outside the scope of lawful purpose and could be non-compliant of the UK GDPR and Data Protection Act 2018, including elements of the Human Rights Act 1998. Consequences: Data captured may contain personal data, as set out in Article 4 of the UK GDPR but may also contain general data. As the CEO is unable to view the footage and given the device is docked at the end of their shift, there would be little benefit in doing this and once detected is likely to result in disciplinary action for the officer. The data itself will be purged once detected. Furthermore, depending on what has been captured the matter may be referred to the authorities for prosecution. Compliance: It would depend on what has been filmed and whether this includes personal data or special categories of personal information. Filming in the public space in general without the presence of personal data is not strictly unlawful. Where that data includes personal data as set out in Article 4 of the UK GDPR then it is subject to data protection regulations, with a lawful basis for processing under Article 6 will be needed. Filming persons in their private dwellings would be an infringement of Article 8 of the Human Rights Act 1998. Once the data has been detected it will be purged and therefore the breach will be minor in impact. However, there is some reputational damage for both Marston and Camden as joint data controllers.	Rare	Minor	Low
Lost or stolen BWC device which is subject to a physical data breach. In this scenario a BWC has been stolen or found and the person undertakes a	Rare	Minor	Low

dissemble of the device to extract the storage device. Consequence: It would depend on the following outcomes: • There is no data saved on the VB400, personal information or otherwise, in which case extracting the storage device would not impact on privacy. If the device is claimed by a member of the public, while in their possession the device could be used irresponsibly, but as data cannot be extracted through normal means, the impact to privacy here would also be negligible. • There is data saved on the VB400, which may contain personal data, and the person(s) manages to dissemble the chassis using hardware tools and retrieve the storage device. As the data is encrypted at source, the footage would not be viewable unless that person also had access to the appropriate installation of VideoManager software, including the unique decryption key. Compliance: While it may be theoretically possible to extract the storage device in this manner, as the data has been encrypted at the source by the VB400 using a unique encryption key, it would not be possible to view any footage without the relevant decrypt key. In this circumstance, reasonable steps have been taken to protect any personal data which accords to the requirements of the Data Protection Act 2018 and UK GDPR. It should also be considered to extract data and attempt to view footage in this manner would mean circumventing protective measure put in place, on the device, through the software and may mean a number of offences are committed include Section 170 of the Data Protection Act 2018.			

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?**
Inherent privacy intrusion where the BWV records a person without consent including audio.	Marston will have in place protective measures: • All CEOs will be trained on the use of BWC, the risks, issues and protocols associated with the devices. • Marston's will ensure that code of conduct and best practice is followed where possible and incorporated this into protocol. • Verbal warning will be given prior to activation which should draw persons attention to the possible activation. This will be further supported by clear labelling on the device, physical indicator and an audible alert. • Auditing of captured data will also be undertaken to ensure compliance with these requirements. • Lastly, it's worth noting that activations are only in response to threats aggression or violence, which should before BWCs was averaging around 22 cases a year.	Reduce Likelihood	Negligible	Yes

	Collectively, the above mitigation should limit the impact to privacy.			
Unauthorised release of data	Access to the data is subject to protective measures and controls, which would limit opportunities for unauthorised data releases: - All officers provided with BWC equipment or who have access to the data, will have received comprehensive training concerning legislation and regulatory requirements, codes of conduct relevant to the industry and UK GDPR. - A limited group of persons have access to the data. - Access to data and its release is monitored by Marston's audit and legal teams. A person would need to login to the software using their credentials and this creates a digital fingerprint which could be used to identify the culprit. This should act as a good deterrent against such actions. - Data which is provided under SAR requests will only be accessible by a unique encryption key, without the key the data would be useless. - Camden and Marston have processes in place to monitor data access, which can be used to trace any unauthorised releases. Collectively, the opportunity for unauthorised data releases should be low as consequence.	Reduce likelihood	Negligible	Yes

Failure to advise persons of BWC activation	CEO will be required to give a verbal warning on any occasion the BWC is activated to comply with the need to reduce the impact to privacy. However, this is not a legal requirement and failure to deliver the warning would not be breach of regulations or adversely impact privacy. The following set out mitigation: • A SOP will be developed for the use of BWC (protocol) which will be provided to CEOs. • All CEOs and persons who have cause to access captured data will be provided training, this will cover the risks, issues, and compliance with data protection requirements. • The BWC is clearly labelled to advise it records both "audio and video" for visual prompt/recognition. • All activations (captured data) will be reviewed by Marstons as these relate to serious incidents on street, and any divergence from the agreed protocol will be followed up with disciplinary action. • Marstons and Camden will review the protocol and determine if positive changes can be made to further mitigate impact on an annual basis. Collectively, the opportunity for unauthorised data releases should be low as consequence.	Reduce likelihood	Unlikely	Yes
Recording without consent or lawful basis.	CEOs will be trained to only use the BWCs in limited circumstances and advised of the risks of doing otherwise.	Reduce likelihood	Negligible	Yes

	- CEOs will be required to give a verbal warning when recording, which is designed to raise awareness of the BWC by the public. - BWC devices are overt and clearly labelled with 'WARNING audio and video recording' which is a visual prompt. When activated the device gives a physical and audible warning. - CEOs will be trained on the use of the device to prevent accidental recordings. - Marston will review the captured data and any non-compliance with the protocol will be subject to disciplinary action. The above controls should help to prevent any incidences.			
Lost or stolen BWC device which is subject to a physical data breach:	The BWC device is not network enabled from a data capturing point and that means it not possible to initiate a remote data deletion protocol. Instead, the device relies on physical and software protection to prevent data interception. However, even with level of protection a person with the appropriate skill, knowledge and experience in electronic devices could undertake a full disassembly of the BWC using commercially available tools and parts. In such a situation, the protection would be defeated and access to the storage drive and data possible. Camden will require Marston to use 'authenticate protection' (encryption of data) on the storage drive. However, this is not set by	Reduce likelihood	Unlikely	Yes

	default by the vendor and will need to be potentially phased in as BWCs are deployed			

Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*
Low

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	**No.** Sarah Laws, Data Protection Manager
DPO advice	Approved, Andrew Maughan DPO June 2023
Information Asset Owner acceptance of residual risks	Peter Mardell, Head of Parking Services
This DPIA will kept under review by:	[redacted] Operations Officer

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	Wilful 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