DATA PROTECTION IMPACT ASSESSMENT

HTTPS://LBCAMDEN.SHAREPOINT.COM/:X:/S/ENVIRONMENTSERVICES/ECXBUHQ5DAVBL2ZICPCCYGWBE28UY_I_PKAKE0BG_YU5G?E=H8RHXE

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	**Kingdom Project**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted] Principle Environment Services Officer on behalf of [redacted]
	IAO name and asset	Rachel Bailey Head of Environment Services
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail. Explain any acronyms on first use.*	London Borough of Camden currently operates an Environmental Education and Enforcement Team, which operates across the borough focussing on littering, dog fouling and waste dumping offences. This resource is limited and so this report seeks approval for increasing the scope and scale of Camden's environmental enforcement capabilities through the use of contract with Kingdom Services Group Limited. Joining the contract, led by London Borough of will permit Camden to increase environmental enforcement personnel for hot-spot area enforcement and night-time enforcement of waste dumping and littering. This service will benefit the Council by increasing enforcement resources alongside the comprehensive administration of fixed penalty notice (FPN) issuing and management, and so supporting the objective of clean streets. To provide enforcement against acts of environmental crime on behalf of Camden Council. The aim of the service is to change behaviour towards environmental crime through education and enforcement including issuing fixed	

	penalty notices (FPN) to offenders. There will be a team of officers issuing FPNs for crimes such as littering, dog fouling, fly tipping and waste duty of care offences Data is collected from individuals who commit environmental crime offences and used to prepare prosecution files in the event of non-payment of an FPN. It is envisaged that data will be collected from around 4000 individuals per year. The service provider (third party) will provide and maintain all systems and equipment used to deliver and manage the service. A FPN is updated on a PDA handheld printed in the presence of the person who receives a copy. The electronic copy of the data is encrypted and sent back to the LAS data store where is can be accessed on their dashboard.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	24th January 2022, revised 24th January 2024

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Please see DPIA Pre assessment form for sections 1 & 2

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	NO
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	NO
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	NO
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	NO
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	NO
1.6	Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	YES
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	YES
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	YES

1.9	Will data be combined, compared or matched from multiple sources?	YES
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	NO
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	NO
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	NO
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	NO
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	NO
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	YES
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	NO

Step 2: What personal data is being used?										
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New/Changed			
							Already happening passed to new contractor as a responsibility.			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	**Y**	Date of Birth	**Y**	Gender	**Y**	National Insurance Number	**N**	Financial Information about the person	**Y**
	Address	Y	Email address	Y	Telephone number	N	NHS No	N	Other eg a reference number such as Mosaic ref	N
	Other data *(Please state):*		*We obtain criminal case result data and reference numbers*							
	Special Categories of Personal Data									
	Racial or ethnic origin	Y	Fingerprints/ Biometrics	*N*	Religious or philosophical beliefs Political opinion				*N*	
	Trade Union membership	N	Physical or mental health or condition						Y	
	Sexual life or sexual orientation	N	Housing records Social services records	N	Tax, benefit or pension records	N	Employee/HR records		N	

	Other data *(Please state):*	
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Yes – past offences related to the issued FPN or prosecution – repeat offences

Step 3: Describe the data processing

3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared?**	Body camera data worn by the officers undertaking the enforcement work. The cameras are encrypted and cannot be accessed if intercepted or stolen. Kingdom officers have EDAs for issuing enforcement notices. They have manual upload as a backup and Wi-Fi upload of all encrypted data. Data is passed via the AWS to the Cloud in encrypted format. Camden officers must request access via LAS system only. All data is stored and processed by Kingdom. Search software legal LAS database. Kingdom employed officers in Environment Services will only use this system to conduct searches that relate to FPNs issued or legal processes they are undertaking. Kingdom officers can search by FPN number and last name to obtain legal data evidence, address, and date of birth data, notes. Other Camden sections request to Environment Services for information and obtain data directly from Kingdom's Information officer, unless the data has already been passed to Camden officers in Environment Services. Camden data searches requests, Camden employed officers may be passed data from Kingdom LAS system in CSV/PDF format via protected email which is then reviewed and checked against legally available personal data within the environment Services section or further passed to Camden's legal department only. This is only to pursue legal obligations for FPN issue or prosecutions or complaints handling. Camden held personal data is not passed to Kingdom. Kingdom data is restricted by user and password timed access to software systems data, staff undertake pretraining to access the data, the systems hold or retain all confidential data and have the built ability to interrogate to retrieve data extracts to provide relevant data only. Relevant data on past FPN'S, gender, Address and postcode, offences, and notes. Super-Users as technical controllers are in place to interrogate officer accessed data and all data retrieval is audited every 6 months. Electronic and paper-based information can be extracted in password protected PDF and CSV formats and emailed to Camden officers. Camden officers are trained to receive the data via Camden's secure encrypted email system which uses sensitivity labelling here . Data received and held is only reshared with Police, Crime or legal Camden services under legal requirement and due process. Process maps (See S 3.4) for the non-digital limited use of data is restricted and content disposed using our confidentiality destruction manual processes including shredding any printed material. Temporary content is deleted after 31 days except if marked for prosecution and legal process. Content is held for the duration needed for legal requirement and then deleted or destroyed. Camden's file management is stored under password protected and restricted server accessed folders as set up with Education and Enforcement or Legal services file. administration.

<table>
<tr><td>3.2</td><td colspan="2">Explain in as much detail as possible why this is being done</td><td>

Legal evidence checks
Complaint's handling
Contact information access
Legal and prosecution evidencing offences and past offences.

Camden is following legal and administration processes to manage the issue and to pursue FPNs and other legal prosecution evidence required in the event of taking further legal action or due diligence against an offender or alleged offender for breaking the law in relation to enviro crimes and EU and UK waste legislation under the EU Waste Framework Directive and specifically, as set out within the legal Kingdom Local Authority contract under Schedule 8.

We require address-based data. Gender and D.O.B data.
We require evidence of past non-compliance under legal investigation or where similar contraventions exist.
</td></tr>
<tr><td rowspan="4">3.3</td><td colspan="2">Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td>Yes - Kingdom will be managing the LAS information retrieval system and camera footage evidence data storage software for which content extracted is passed back to Camden in the right CSV or PDF format for accessing controlled data sets as required for data record keeping or further legal evidencing under Camdens web and IT servers security within Environment Services. Data Centre Plus retain all Kingdom web software and IT data retrieved by Kingdom officers and undertake penetration tests to ensure the information is securely obtained under their ISO27001 certified data centre .</td></tr>
<tr><td>External organisation or partner Name</td><td>Controller or Processor?</td><td>Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection? Yes/No/In progress</td></tr>
<tr><td>Kingdom Services Group LTD</td><td>Controller and Processor</td><td>Yes formal joiners contract from 2022 Jan 24th, updated and reviewed on 24th January 2024</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

3.4.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**	Yes - For the camera footage access, paper based data use and electronic stored data within Kingdom server systems. https://lbcamden.sharepoint.com/:p:/s/EnvironmentServices/EUQ5qv4xhH1GjiRFGxneSv0BkKe03-HVCv9_rbtHR0EEUg?e=cZofAD https://lbcamden.sharepoint.com/:w:/s/EnvironmentServices/EYInypNZ0dFDkz_Ql7GzE1cBGLCyYVcecaFIUELuboVEeA?e=72yuvY
3.5	**How will the information be processed/shared. Details eg secure file transfer**	CSV file transfer for any vetted address based or personal data or legal documentation to be shared with Camden officers or legal teams. Camera footage is not accessed by Camden directly, however, may be externally retrieved by national Police and crime investigation bodies under their security and surveillance legal permission processes working directly with Kingdom. Training on use of accessed software for Camden and Kingdom officers is Managed by Beta who is Kingdom's Developer.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition Our legal basis for processing is Article 6(1)(b) – that the processing of personal information is necessary for the performance of a task carried out in the public interest, and 6(1)(c) for legal duty.	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article (9)(2) (g), that there is a substantial public interest based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Art 10 requirements by having art 6 legal basis as identified above, and the schedule 1 condition for processing criminal offence data is the same as identified for art 9(2)(h).
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**		
	Under Contract for Information Security and GDPR protocols including data subject rights, under DPIA approval, Under Supply Chain Assessment for IT and web application access.		
4.3	**How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		
	This is covered in the pre-screen and under Section 3.1		
4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Processing Notice online		Yes

4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**
	YES
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject
	No – We gather legal evidence that is pertaining to gender, age and photo evidence within footage or Camden known character referencing. Kingdom data is passed to Camden Education and Enforcement team securely and may then be redirected to legal or prosecution services as evidence.
4.7	**Data Retention Period - how long will the data be kept?**
	The maximum storage of data will be 6 years. The minimum storage of data will be 1 day. Data is only retained if required for legal processing and administration purposes. Data used for pre-checking for alleged prosecution purposes is deleted within 1-4 weeks. Data passed to Camden for file for legal submission on a live prosecution may be kept for 4+ weeks and will be deleted within 6 months unless legal require it to be retained. Data – stored on the Camden Environment Services E&E data files to be passed to legal within 4 weeks to 6 months. Data non-personal may be viewed and used to evidence for a FOI or ERI. Data requested by legal not readily available on the E&E data files requested by legal will be requested separately to Kingdom as an external request for personal data.
	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.*
	Local Authority Support (LAS) System – Backoffice – Kingdom **Halo Vault – Kingdom** **SharePoint** - https://lbcamden.sharepoint.com/sites/environmentservicesmigrated/Education%20%20Enforcement%20Cases/Forms/Document%20set%20Limited.aspx **Camden Environment Services.** **Limited to members of the Education and Enforcement trained team**
5.2	**Where is the data stored geographically?**
	In the UK, Manchester.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	Kingdom Camden Employees and Kingdom Management, Education and Enforcement Officers, the Education and Enforcement Manager, Legal Administration Teams within Camden, or where legally required Police and Criminal Investigation Bodies within the UK.
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Please see 3.1, 3.3, 3.4 **Local Authority Support (LAS) System – Backoffice – Kingdom officer, management, and admin officer** **Halo Vault – Kingdom – Camden admin/ Team Leader and Kingdom officer and management -** **SharePoint (Include url) Camden Environment Services. Camden Enforcement officers and management - password protected / encrypted emails**
5.5	**Is there an ability to audit access to the information?**
	YES

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?**
	All data is dual encrypted. Only PDF/ CSV formats. Training in GDPR. Behavioural training on induction Talent LMS awareness course. Audits every 6 months, manual spot checks, review of destruction process, ICO request reviews for flagged (Kept data). Automated closure of screen access after 2 minutes. Regular penetration tests by IT leads, firewalls, hacking evidence.
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Information security have reviewed the security measures and all questions have been answered. Reviewed by [redacted] Category Manager IT Service

Step 6: Identify and Assess Risks

Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. Please refer to DPIA tab. https://lbcamden.sharepoint.com/:x:/s/EnvironmentServices/EcXbuHq5daVBl2ZiCPCCYGwBe28uy_i_PKaKe0Fbg_yu5g?e=h8rhxE **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm-see table 1**	**Severity of harm-see table 2**	**Overall risk – see table 3**
***Misuse of data**; Personal data could be used in a manner incompatible with the Data Sharing Agreement. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.*	*Unlikely*	*Major*	*Low risk*
Privacy Intrusion The anguish or suffering can happen if a privacy intrusion incurs, such as filming an individual without good reason.	Unlikely	Moderate	Low risk
E*xternal illegal IT access to stored data information*	Unlikely	Major	Moderate/Medium risk

Deliberate Inappropriate use of data access for bias or harassment of an individual.	Unlikely	Major	Low risk
Loss or damage to the EDA device The EDA device is used by the LAS officer to input personal data (Name, address) to populate and print the FPN ticket. The risk is where there is a possibility of an EDA being lost during the course of an officer's duties or damaged in an altercation.	Possible	Minor	Low risk
Unauthorised access, loss, processing of LAS system held data Full details of the ticket issued, the environment offence concerned and any correspondence between LAS Administrators and the offender are stored on this system. The risk is that an LAS officer could, inadvertently or maliciously leave the data be exposed or gain access for purposes outside the set list of reasons given to enable processing.	Rare	Major	Low risk
Loss or damage to the BWC device The BWC device is used by the LAS officer to record their interaction with members of the public during the course of a ticket being issued. The camera may therefore will record a physical image of that person which will reveal race and possible disabilities. It can also include discussions of an alleged criminal offence. The risk is where there is a possibility of a BWC being lost during the course of an officer's duties or damaged in an altercation.	Possible	Moderate	Medium Risk

Step 7: Identify Measures to reduce risk				
Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.* Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by IRT/DPO* The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.				
Risk identified in step 6	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved?**
Misuse of data; Personal data could be used in a manner incompatible with the Data Sharing Agreement.	The system controls to limit access to data is minimal through encryption and other IT certifications and penetration tests. The main routes for data misuse are behavioural or officer intercepted means, training and induction and recruitment expertise is in place for officers. Options include refresher training, management monitoring of access and street-based activity and data destruction processes for data no longer required.	6 month audits of LAS and HALO system officer use by Managers/ External Penetration Testing by IT teams / external audits Training GDPR awareness – e-learning modules. Limit paper and print, destruction process in place and officers trained to use.	Residual risk of embarrassment / reputational damage to Camden council / LAS remains if information is exposed and used for detriment.	HOS Reviewed 13/1/24

Privacy Intrusion	BWC can only record footage when manually switched to record by an officer. Recording stops when the BWC is manually switched off. In the unlikely circumstance a BWC is accidentally knocked into the on position the BWC would record footage for 30 mins before uploading. The footage can only ever be uploaded to the HALO cloud, where it is not accessible to anyone other than the designated administrator / team leader. LAS administrators check daily for any miscellaneous footage captured that is not part of an FPN interaction. Any footage of this nature is deleted. LAS takes views any purposeful and malicious acts of privacy violation as an act of gross misconduct. Officers suspected or alleged to have committed privacy violation will be subject to a full investigation and be sanctioned appropriately.	Training GDPR awareness – e-learning modules. Training on the correct use of BWC given on induction Holding strap for BWC positions the camera in a place where accidental turn on is unlikely Daily audits by LAS admin for miscellaneous footage	Residual risk of embarrassment / reputational damage to Camden council / LAS remains if information is exposed and used for detriment.	HOS Reviewed 13/1/24
E*xternal illegal IT access to stored data information*	Camden servers have been limited and secured access through encrypted laptops / PCs. In the event of loss or theft, the laptop can be locked remotely by Camden, and access to the servers can be removed from a specified account. GDPR awareness training, focusing on behavioural awareness surround data sources and processing is mandatory for all employees and must be completed ever 12-18 months. Access is restricted to the LAS Admin, LAS Team Leader for site and LAS Business Manager for the contract.	The physical measures in place to secure the device reduce the likelihood of harm to Unlikely / Rare, The impact stays at major due to the information available on the LAS back office system	Residual risk of embarrassment / reputational damage to Camden council Reputational risk to member of public being processed for an environment offence due to their privacy being impacted.	HOS Reviewed 13/1/24

Deliberate Inappropriate use of data access for bias or harassment of an individual. / Invasion of privacy.	The main point of access to data is via the PDA screen, by theft of the cameras on officer's work wear, the viewing of screen data within an office or home working environment or on street. The main concerns for accessing data presented in a format that reveals personal data could be behavioural and includes the following: payment or fraudulent offers to staff to share data, illegal viewing or screenshots taken of data, coercion, or manipulation of officers through persuasion or false intention in order for information to be shared. Invasion of privacy, deliberate intent to cause intrusion or harm by undertaking a surveillance activity or using position or equipment to gain access to privacy in a way that deliberately intrudes and harms another person. This can be by filming someone, accessing their personal data where the person is aware of this action being taken. Such cases are limited to known relationships between staff and public and employment screening, regular training and reporting and monitoring of times of access to private data.	Camden and Kingdom employed officers undertake annual refresher training for understanding fraudulent behaviour and how coercive activities can occur. Criminality checks are carried out for all Camden and Kingdom employed staff. Camden and Kingdom Robust reporting and whistle blowing systems are in place for officers to confidentially report seen behaviours or activities that are suspicious. All data that can be accessed it restricted and screens and PDA's timeout after 2 minutes. All staff are trained to close computers and screens when not in use. Camera data is encrypted securely, and encryption is penetration tested for hacking or interception.	Residual risk of embarrassment / reputational damage to Camden council Reputational risk to member of public being processed for an environment offence due to their privacy being impacted.	HOS Reviewed 13/1/24
Loss or damage to the EDA device	The devices are held in reinforced cases to prevent damage. The cases are secured to the vest of the enforcing officer. Each individual device is assigned to an officer at the start of each shift. And must be checked back into the team leader at the end of their shift. The Team leader	The physical measures in place to secure the device reduce the likelihood of harm to Unlikely / Rare. The impact remains minor due to lack of access to the corresponding database even if a device is stolen.	Residual risk of embarrassment / reputational damage to Camden council / LAS remains if a device is stolen.	HOS Reviewed 13/1/24

	will then secure the devices into a locked cabinet. Each device is dual encrypted. A unique site login code and a Unique officer password is required to open and use the devise. The device does not hold any data on it once a ticket has been printed, as this is sent to the cloud. In the event a device is stolen before a ticket could be printed the information on said ticket is restricted to basic PII – name and address, and the category of environmental offence observed.			
Unauthorised access, loss, unlawful processing	LAS Back Office system has limited and secured access through encrypted laptops / PCs. In the event of loss or theft, the laptop can be locked remotely by Kingdom IT, and access to LAS can be removed from a specified account. Persons processing LAS data and issuing tickets are subjected to appropriate vetting standards and criminality checks before employment. GDPR awareness training, focusing on behavioural awareness surround data sources and processing is mandatory for all employees and must be completed ever 12-18 months. Access is restricted to the LAS Admin, LAS Team Leader for site and LAS Business Manager for the contract.	The physical measures in place to secure the device reduce the likelihood of harm to Unlikely / Rare, The impact stays at major due to the information available on the LAS back office system	Residual risk of embarrassment / reputational damage to Camden council / LAS remains if access is gained an information is made public. Reputational risk to member of public being processed for an environment offence due to their privacy being impacted.	HOS Reviewed 13/1/24

Loss or damage to the BWC device	The BWC devices are held in reinforced cases to prevent damage. The cases are secured to the vest of the enforcing officer. Each individual device is assigned to an officer at the start of each shift. And must be checked back into the team leader at the end of their shift. The Team leader will then secure the devices into a locked cabinet. Each device is dual encrypted. A unique site login code and a Unique officer password is required to use the devise. Footage cannot be played back on the camera alone, it is uploaded to the cloud via a secure wifi / 4g connection. In the even to of an upload failure a manual check and upload can be done by tethering the camera to the corresponding PC. A manual check of possible footage is done as standard procedure at the end of each day. Access to any footage is only possible through the HALO vault database which requires unique passwords to access. Access is restricted to the LAS Admin, LAS Team Leader for site and LAS Business Manager for the contract. BWCs can also be disabled remotely in the event of loss of theft	The physical measures in place to secure the device reduce the likelihood of harm to Unlikely / Rare. The impact remains minor due to lack of access to the corresponding database even if a device is stolen.	Residual risk of embarrassment / reputational damage to Camden council / LAS remains if a device is stolen.	HOS Reviewed 13/1/24
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**	Tanya Bryant DPO, Sarah Laws DPO, Andrew Maughan DPO, [redacted], Camden, [redacted], [redacted] and [redacted]
DPO advice	Completed
Information Asset Owner acceptance of residual risks	Rachel Bailey Head of Environment Services
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted] Engagement and Enforcement Manager and [redacted] Principle Environment Services Officer

Version Control

Version	Reason	Date	Author(s)
1.0	**Start of new project.**	**13/1/2022**	**Rachel Bailey, Head of Service Environment Service.**
1.1	**Annual Review of project contract**	**24/1/2024**	**[redacted], Education and Enforcement Manager.**

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

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

Table 4: is the risk

15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

level acceptable?

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) Camden Council's Data Charter (sharepoint.com)

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?)*

- Camden's streets, like many inner-city areas, suffer from some residents and businesses dropping litter and dumping waste that negatively impacts on; the borough's environmental cleanliness; people's experience of an area, and feelings of safety. It is important that those who commit environmental offences meet the consequences of their actions and change their behaviour.

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

By tackling waste dumping, fly-tipping and littering we will support the core aims of Camden 2025 and Our Camden Plan including maintaining "clean, vibrant and sustainable places".

- Failing to meet the core aims of the 2025 plan
- Increased feelings of being unsafe in public areas
- Negative public environments and much more grime

- Increased fly tips and hazardous dumping of rubbish
- No legal compliance or following of due process under law

2. *Data Bias*

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

- Evidencing access, times of use, and users against data retrieved and checking this is valid and appropriate under current cases for legal action

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?*

- Managed under the Camden disciplinary processes in conjunction with Kingdom's disciplinary processes.

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**?

- Persons with past crimes that have been spent or criminal associations and perceptions of offenders
- Anybody who identified and has a protected characteristic under Equalities

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?*

- We follow legal data compliance legislation
- Staff are qualified and accredited to handle and manage the data as legal enforcement officers.
- Staff continue to attend training sessions and information awareness courses.
- Staff comply with Camden's employment and induction training on data protection and GDPR.

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**)*

- LAS System is designed to only draw and filter relevant data from legally appropriate sources for interrogation and data requests.
- Limits to the types of requests and request instructions are pre set to help ensure no mis-management of personal data extraction.
- Footage data meets the surveillance and image data compliance and is stored securely, and access is restricted, it's encrypted if shared and follows request protocols for authority to be disclosed for legal evidence use.

ii) *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**)*

- *All metadata and field names clearly understood and software under appropriate licence*

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

- Camden could increase the number of street-based officers 24 hours 7 days per week to deliver adequate visible presence to act a deterrent to waste related crimes and offences. This would equate to 1 officer per ward. Camden would not seek to apply any legal action for waste crime. Camden has increased its contractual management and service delivery of cleansing, waste control and disposal.

	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
IMPACT	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