DATA PROTECTION IMPACT ASSESSMENT

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

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

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

Project Name	Body Worn Video (CCTV) in all services except Parking	
Project Lead and Information Asset Owner/s	Project Lead	Deborah Pyne CCTV Governance and Data Manager (SPOC)
	IAO name and asset	Steve Harris (CCTV Corporate Owner)
	IAO name and asset	
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail.* E*xplain any acronyms on first use.*	Body Worn Video (BWV) cameras are small, visible devices worn attached to the officers' uniform (usually on left, right of cent of chest). Used to capture both video and audio evidence when officers are attending all types of incidents. BWV issued to Responsive Security Patrol, Enforcement and Community Presence Officers in contact with the public. This DPIA also covers the use by Security if/when this becomes live. The purpose is to record enforcement, investigative and other encounters between the RSP/ Enforcement and Community Presence Officers /Security officers and the public. There is an existing DPIA since 2021, this DPIA is updating the previous one and moving onto a new template. The processing is continuing. BWV is used for: • when arriving at a location either through pro or reactive patrolling for Community Presence, ASB, and Environmental Officers to capture environment/activity • activate for personal security when approaching or being approached by one or more persons	

	• activate to support RSP patrolling reports uploaded to Northgate where applicable • for RSPs only: activate with permission of resident if required when conducting welfare tenancy checks in a person's property • recording interactions where necessary to obtain evidence
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	Ongoing- this is an update DPIA

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

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

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	no
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	yes
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	no
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	no
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	no
1.6	Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	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?	no
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
1.9	Will data be combined, compared or matched from multiple sources?	no
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	no
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	no

1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	no
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	no
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	no
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	yes
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	no

Step 2: What personal data is being used?												
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New/Changed					
							Unchanged					
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate											
	Personal Data											
	Name		Date of Birth		Gender		National Insurance Number		Financial Information about the person			
	Address		Email address		Telephone number		NHS No		Other eg a reference number such as Mosaic ref			
	Other data *(Please state):*		CCTV footage – visual and audio recordings of person and behaviour, speech									
	Special Categories of Personal Data											
	Racial or ethnic origin	y	Fingerprints/ Biometrics		Religious or philosophical beliefs Political opinion					y		
	Trade Union membership		Physical or mental health or condition							y		
	Sexual life or sexual orientation		Housing records Social services records		Tax, benefit or pension records		Employee/HR records					
	Other data *(Please state):*		Only where this is disclosed verbally on a recording or where it is obvious from visual recording eg presence of religious clothing/head wear/ obvious visible disability.									
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?		Only where the recording captures this									

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? Please use plain English!**	Each time the body worn video activated to record an individual(s) the officer operating the BWV must verbally inform those who are being recorded that the body worn video is recording. This verbal notification must be part of the recording upon activating the BWV. Recording activated at the sole discretion of a RSP officer. Data downloaded after each RSP officer shift (daily) by a SIA CCTV licensed Operator. Downloads carried out in restricted access – CCTV Hub at Holmes Road Depot within the CCTV control review room. Data downloaded onto Pinnacle cloud software (independent software owned by third party) with individual usernames and logins. Data remains on software system storage for 31 days before automatic erasure. Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Footage required for investigation, a copy of the recording saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required.
3.2	**Explain in as much detail as possible why this is being done**	Purpose: to record enforcement, investigative and other encounters between the officers and the public. Deterrent for personal officer attack Deterrent for activities of continued anti-social behaviour, group gathering in communal areas Security tool in the event of personal officer attack Supporting data with generated report for housing officers and partner agencies to progress cases Reassurance to public and third parties measures in place reducing risk – public interest Accountability for interactions

<table>
<tr><td></td><td colspan="2"></td><td></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</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>Pinnacle (equipment provider)</td><td>Processor</td><td>contract</td></tr>
<tr><td>Met Police (where offences occurred)</td><td>Controller</td><td>Yes, suite existing DSAs</td></tr>
<tr><td>3.4.</td><td colspan="2">Please explain your process from start to finish. you can do this is a diagram if you wish, or a flow chart, or describe it. You can attach a document if that’s easier.</td><td></td></tr>
<tr><td>3.5</td><td colspan="2">How will you handle data in your project, how will use store and share it. Please explain</td><td>Recording activated at the sole discretion of a RSP officer. Data downloaded after each RSP officer shift (daily) by a SIA CCTV licensed Operator. Downloads carried out in restricted access – CCTV Hub at Holmes Road Depot within the CCTV control review room. Data downloaded onto Pinnacle cloud software (independent software owned by third party) with individual usernames and logins. Data remains on software system storage for 31 days before automatic erasure. Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Footage required for investigation, a copy of the recording saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required.

Sharing with Police through existing well established disclosure provisions and channels.</td></tr>
</table>

<table>
<tr><th colspan="4">Step 4: Assess lawful basis, necessity, and proportionality</th></tr>
<tr><td>4.1</td><td colspan="3">Identify the Lawful Basis for processing personal data/special category /criminal data.
If you don't know then please ask Data Protection Advice Team for advice (DPA@camden.gov.uk if you have no named Information Rights Officer advising) If not processing the category say N/A</td></tr>
<tr><td></td><td>Personal data Article 6(1) UK GDPR condition

For safeguarding information and personal safety (c) legal duty

For welfare checks in tenant's property ONLY (Unless operative records for their safety where it is (c)) (a) consent

All other usage: (e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.</td><td>Special Category data UK GDPR Art 9 condition and DPA18 schedule condition
For all processing (except welfare checks in tenant's property where operative not recording for their safety) (g) substantial public interest. The DPA 18 Schedule 1 Part 2 conditions being para 6 Statutory and government purposes and the underlying law being Care Act 2014, Children Acts, Health and Safety at Work etc Act 1974 and the various laws the operatives enforce (eg Environmental Protection Act 1990) and para 18 safeguarding with the underlying law being Care Act 2014, Children Acts

For welfare checks in tenant's property ONLY (and where operative does not record for their safety) (a) explicit consent, provided verbally</td><td>Criminal data UK GDPR Art 10 condition and corresponding art 6 condition

For criminal offence data the article 10 requirements are met by the art 6 conditions as for personal data and the schedule 1 conditions as for special category data</td></tr>
<tr><td>4.2</td><td colspan="3">If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Data Protection Advice Team have advised this is appropriate</td></tr>
<tr><td></td><td colspan="3">For welfare checks in tenant's property ONLY (and where operative does not record for their safety) (a) explicit consent, provided verbally and recorded on the BWV footage</td></tr>
<tr><td>4.3</td><td colspan="3">How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims? If this is covered in a pre-screen refer to the pre-screen, otherwise detail below</td></tr>
<tr><td></td><td colspan="3">Accuracy is provided by it being a live recording.

Recordings are not continuous and only activated to record on a positive action by the officer deploying the BWV.</td></tr>
</table>

4.4	**Have/ will 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 Privacy Notice? Remember telling people is not the same as asking for consent	Yes. Officers wear the BWV visibly and each time it is activated to record an individual(s) the officer operating the BWV must verbally inform those who are being recorded. This verbal notification must be part of the recording upon activating the BWV.
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes.	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject.	
	No.	
4.7	**Data Retention Period - how long will the data be kept? What will happen to the data at the end of the project – deleted or kept? If you're using a processor what are the arrangements with them for data at the end of the project?**	
	Data remains on software system storage for 31 days before automatic erasure. Where footage is required for investigation, a copy of the recording is saved onto the Camden PC hard drive and released following all existing CCTV data management protocols for the CCTV Hub control room. Data saved manually deleted once the data is no longer required, periods for which will vary depending on the actions undertaken.	

Step 5: Information Security Process	
5.1	**On what systems will the data will be stored** *Examples include Mosaic, SharePoint, shared drives,*
	Pinnacle system. Retained footage on Camden PC hard drive.
5.2	**In what country is the data stored?**
	UK
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	CCTV Data and Governance Manager
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Yes
5.5	**Is there an ability to audit access to the information?**
	Yes
5.6	**What security and audit measures will there be to make sure that data is kept safe?**
	Downloads carried out in restricted access at the CCTV Hub at Holmes Road Depot within the CCTV review control room. Data downloaded onto an independent PC onto Pinnacle cloud software with individual usernames and logins. Data remains on software system storage for 31 days before automatic erasure. Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Where footage needs saving for investigation a copy of the recording is saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required. The third party software used to store data to cloud has no footprint on the Camden network.
5.7	**Has the Information Security Team advised on the security measures? What were their comments?**
	Yes, cleared in 2021 and unchanged since

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary.	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
CCTV unauthorised recorded data obtained by third party. Live and or recorded CCTV data of identifiable person(s) and their associated activities released without authorisation in public domain. • 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 • The potential of the individual's need to relocate to another residence • Possible inadmissible evidence for prosecution • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual	Possible	Medium	Medium High
Inherent privacy intrusion from BWV which records a person without consent including audio. Privacy intrusion, loss of control over data, embarrassment distress	Likely	Medium	Medium High
Retaining data beyond retention period. Privacy intrusion, loss of control over data.	Likely	Medium	Medium High
Sharing excessive footage with 3rd parties. Privacy intrusion, loss of control over data, embarrassment distress	Likely	Medium	Medium High

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 /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?**
CCTV unauthorised recorded data obtained by third party.	Pinnacle system is designed so that Operators are unable to delete or manipulate any data. RSP reports clearly state if a BWV activated and each report matched to the BWV recorded footage. Officers cannot access footage themselves. Only designated roles have access. Where footage is required for investigation, a copy of the recording is saved onto the Camden PC hard drive and released following all existing CCTV data management protocols in line with previous DPIA documents for the CCTV Hub control room. Data saved manually deleted once the data is no longer required. Access to the PC covered by existing policies and procedures, with RBAC. Staff SIA Licenced/trained with annual re-fresher training, licenced and police vetted (NPPV1), knowledge of data handling. Obtaining or releasing unauthorised data could lead to disciplinary actions	Reduced	Low	Yes
Inherent privacy intrusion	Recording is not constant but undertaken by a positive act by operative when required by a situation. Operatives are trained appropriately, as to when BWV is used. This reduces amount of footage and ensures that only necessary footage recorded. Public now generally accept that BWV is used. Since 2020 there have been no complaints received about the use of BWV (it is believed there were none prior to that date either) indicating privacy intrusion is not a serious issue. The highest intrusion is within people's homes. This is the minority of recording and undertaken for example for welfare checks. In	Reduced	Medium	Yes

	those cases, consent sought to reduce intrusion. Where the operative feels recording is necessary for their health and safety then consent overridden. In this case, a small minority of cases, the intrusion deemed acceptable in terms of safeguarding the operative's safety. Footage obtained is stored securely, accessed and used for legitimate reasons only.			
Retaining data beyond retention period.	Pinnacle system has automated 31-day deletion. Only data downloaded onto laptop for investigation retained longer. This is manually deleted with risk that it will not be done in a timely manner but processes for review are in place.	Reduced	Low	Yes
Sharing excessive footage with 3rd parties.	Officers cannot access footage themselves. Only designated roles have access. Where footage is required for investigation, a copy of the recording is saved onto the Camden PC hard drive and released following all existing CCTV data management protocols. There are existing DSAs with the Police for data sharing.	Reduced	Low	Yes
Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*				
Medium				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO/DPM	No, Sarah Laws, Data Protection Manger
DPO advice	
Information Asset Owner acceptance of residual risks	Names of IAOs Steve Harris
This DPIA will kept under review by: (*usually the author or the IAO)*	Deborah Pyne, CCTV Data and Governance 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)
Medium	*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
	Medium	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 Medium 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