Bolsover District Council/ North East Derbyshire District Council
Privacy Impact Assessment (Stage 2) Version 7 – 10/10/19

Project Manager (include contact details)	Policy: K. Shillitto, Solicitor Implementation: TBC
Project Name	Mandatory CCTV in Taxis
Brief Project Overview - NEW project	The introduction of a prerequisite that all vehicles must have installed functioning CCTV to Council specifications prior to a Private Hire Vehicle licence being granted. The authority will act as data controller for all footage recorded.
Brief Project Overview – EXISTING system (If this is a change to an existing project, system, procedure, technology or legislation, describe the current system and the proposed changes)	N/A
What are the potential privacy impacts?	CCTV recording of individuals, including potential data of sensitive nature. Includes recordings of potential criminality.

Ref	Question	Response	Further Action Required	Date Completed
1.	Personal Data Processing			
1.1.	Which aspects of the project will involve the processing of personal data relating to living individuals?	The project will involve video and audio recording of living individuals (passengers and taxi drivers) by front-line officers in prescribed situations (see below for information on guidance and training)		
1.2	Who is/are the Data Controllers in relation to the processing?	NEDDC is the Data Controller. Senior Managers in	I need to understand how it will work in practice – who actually	

		Environmental Health (Licensing) will have responsibility for policy/procedural adherence.	controls the CCTV system, the licence holder or us? If us how do we protect the privacy of the taxi driver when using his vehicle for personal use The system installed in the vehicle will be operated by the driver, who activates video surveillance when the vehicle is being used for taxi work. Time-limited audio recording will be activated by the driver or passengers using buttons in the vehicle.	
2.	Fair and Lawful Processing			
2.1	Which article 6 condition, and for special category (sensitive personal data) which article 9 processing condition are you relying on?	**GDPR Article 6(1)(e)** (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (Respective privacy statements for the service areas concerned list the relevant statutes and regulations) **GDPR Article 9(2)(f)&(g)**	Need to reference the legislation that is making this mandatory (as it strengthens the public task) In July 2020 the Government published the Statutory Taxi & Private Hire Vehicle Standards, which the authority has a legal duty to have regard to, expects the recommendations to be implemented unless there is a compelling local reason not to. Recommendations include the mandatory requirement for CCTV in taxis. No compelling local reason has been	

		(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of 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. **NB Additional details of the basis for necessary processing are contained in the supporting document.**	identified not to consider this policy.	

		Data Protection Act 2018 Sch 2 Pt 1 (2) (1) Crime & taxation exemption **NB** Some GDPR provisions e.g. to disclose personal data to third parties do not apply when one of the above exemptions is engaged. Also compliance with: ICO data protection Code for Surveillance Cameras and Personal Information Home Office Surveillance Cameras Code of Practice		
2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?	The processing of this personal data is not reliant upon consent (see 2.1) Vehicles will be obliged to carry signage explaining to occupants that CCTV recording is taking place.		
2.3	Is the project covered by existing fair processing information already provided or is new communication needed?	***No***	Consider provision of relevant information on websites for vehicle users to access separately?	

			Existing privacy statement for Environment Health & Licensing will need updating together with clear signage in vehicles and effective publicity informing the public (website, press release, Intouch, social media etc.) Also consider having cards for the taxi driver to hand out if someone wishes to request footage or seek further information. Enquiries and requests need to come to us as the DC.	
2.4	Is the processing in accordance with other legal /regulatory requirements e.g. Human Rights Act.	Yes (see above and supplemental document) and relevant CCTV policies.	Legal requirements and framework is referenced in the CCTV policy. Consider reviewing and including situation-specific guidance. Licensed taxi drivers will be in physical possession of the data storage device. Guidance on proper storage and security will be required.	
2.5	If third parties are involved in the collection of data do they need informing?	Yes to the extent that the physical storage device is stored within the licensed vehicle however the Council (as data controller) will control the purposes for collection.	See 1.2 & 2.4. ~~Who switches the recording on and off? How to we prevent recording when the vehicle is being used for personal use.~~	

			Or conversely how do we prevent the taxi driver switching it off when being used for licensed purposes? Failure to switch the system on while using the vehicle for licensed purposes will be an actionable breach of licence condition.	
2.6	Is there a risk of anyone being misled or deceived?	No, the vehicle signage will be clear and mandatory.		
2.7	Is the processing fair and proportionate to the aim of the project?	Yes, on the grounds of public protection as set out in the supporting document.	As before note the legislation making it mandatory in the supporting document See 2.1	
3. Specified and Lawful Purposes				
3.1	Has a clear purpose for data processing under the new project been identified and documented?	Yes, as per supporting document.		
3.2	Are the notifications to the ICO sufficient to cover data processing under this project?	N/A		
3.3	Are the purposes clear in notices to individuals?	Yes, as per signage above.	Plus updating of privacy statement, use of cards by the taxi driver and updated information on the website	
3.4	How will you ensure that use of personal data is limited to these purposes?	Only trained and authorised staff will process data. Thorough staff training and operational guidance will ensure adherence to stated purposes. Legal advice available where needed.	So noting my earlier questions above - is the intention for the CCTV to record continuously whilst in use for licensed purposes and then to override after X days. How do officers access this information? And I imagine that they will only be	

			doing so for the specified purposes e.g. alleged criminality, data subject access request (DSAR) etc. So a log will need to be kept of these searches and downloads.	
4. Adequate, Relevant and not Excessive				
4.1	What categories of data will be collected?	Video images and audio recording when the camera is operating.		
4.2	Is each category relevant and necessary? Is there any data you could not use and still achieve the same goals?	CCTV will be able to record exactly what happened, what was said and when, in an indisputable format. Their use will be covered by the management processes described in this PIA and staff will receive training and guidance in their use.		
4.3	Can data be anonymised?	***TBC*** - ***Need system info***	Some systems allow images to be blurred. This is useful functionality if someone is requesting their own personal data as it allows other passengers and the taxi driver to be obscured	
5. Accurate and Up-to-date				
5.1	What steps will be taken to make sure accurate data is recorded and used?	Recordings of 'live' situations so it is an accurate record of the exchange between individuals in the vehicle.	Procedure/standards to be established to ensure evidential robustness of the footage for court purposes.	

		Footage to be automatically erased after a period of ***???*** days. Date and time functionality on the CCTV system? ***Need system info***		
5.2	Can records be easily amended?	***TBC*** ***Need system info***		
5.3	Are out-of-date records archived or destroyed?	Yes, automatic deletion after ***14/28*** days unless downloaded for use as evidence in enforcement and/or legal proceedings.		
6. Data Retention				
6.1	How long will personal data be retained?	Up to 7 years if prosecution is likely. Routinely up to ***14/28*** days. Recordings will only be stored using a secure system and only downloaded for court proceedings.		
6.2	How will redundant data be identified and deleted in practice?	The system automatically deletes data after ***14/28*** days unless video/audio data has been identified for evidential purposes in which case it is retained for 7 years.		
6.3	Can redundant data be easily separated from data which still needs to be retained?	Yes, data will only be extracted if it needs to be shown to the court and downloaded onto an encrypted USB, memory device or DVD.		
7. Data Subjects Rights				

7.1	Who are the relevant data subjects? E.g. customers, tenants, employees.	Taxi drivers, vehicle proprietors, passengers.		
7.2	Will data be within the scope of the organisations SAR procedure?	Yes, video and voice recordings, but only if this is requested prior to the automatic deletion period.	***Format of SAR and responsibility for processing TBC*** Happy for my team to administer requests Will need to establish procedure with Licensing for obtaining footage for SARs	
7.3	Is any data processing likely to cause damage or distress to the data subject?	No – the data subject will be aware through signage (and publicity) that CCTV will be recording audio and visual footage.	Need to give consideration on how to communicate this information to blind, partially sighted individuals. Taxi driver to advise in those circumstances?	
7.4	Will there be any direct marketing to individuals?	No		
7.5	Is there any automated decision making?	No		
8.	Data security			
8.1	What security measures and controls will be incorporate into or applied to protect personal data? Consider those that apply throughout the organisation and those specific to the project.	The footage is encrypted by propriety software and only be accessible to authorised officers. Images cannot be deleted by the users. Retention and deletion rules are set up within the system by the system administrator. before using the kit. Access and permissions will be limited to certain named staff	What about the physical data storage in the vehicle? Can this be removed? If stolen is the device itself encrypted? ***Need system info.***	

		and managers who can only view footage in their respective service areas. Footage will be downloaded only in response to a relevant enquiry or complaint. The software contains its own archiving rules, images are usually automatically deleted after ***14/28*** days, unless marked for evidential purposes (i.e. if needed for a prosecution)		
8.2	Is there a need to segregate data? E.g. sensitive data from other data.	***TBC***		
8.3	Who will have access to the data and what controls will be in place?	See 8.1		
8.4	Is there a contingency plan to manage the effects of any unforeseen loss or damage to data?	Downloads will be done solely when necessary and where operationally practical to do so. If the storage device is stolen or damaged before downloaded (and wiped) encryption will prevent access. Images cannot be viewed on the storage device.	To be covered in staff guidance.	
9. Data Processors				
9.1	Are any external data processors involved?	The licence holders (who are storing the device, displaying		

		the signage etc.) and the supplier (s) of the CCTV system (security of device, data transfer etc.).		
9.2	What security guarantees do they have?	***TBC***.	Include links to privacy statements of suppliers and undertakings in place with licence holders	
9.3	Is there/will there be a written contract with the data processors?	***Conditions of licence can be used to set terms for licence holders.***	As this is likely to be the licence holders themselves then a review of the data protection standard clauses would be worthwhile and include in a suitable agreement with the holder as required. SLAs with suppliers.	
9.4	How will the contract be monitored and enforced?	***Licensing enforcement activity will include CCTV***		
10.	Disclosure of Data to Third Parties			
10.1	Will data be disclosed to any other third parties?	Yes, the police, other enforcement bodies and potentially as part of a prosecution		
10.2	Is this third party disclosure fair and lawful?	Yes (see 2.1)		
10.3	What checks have been made on the Third Parties and what data security measures are in place?	Well established 3rd parties involved in law enforcement/justice activities– police, lawyers and courts Appropriate security measures will be used for disclosures to third parties i.e. email	Evidence disclosures to third parties need to be covered in the staff training	

		encryption, hand delivery of footage		
11. Overseas Data Transfer				
11.1	Is there any transfer of data outside of the European Economic Area?	No	Need to check/confirm that when the data is transferred from the storage device to the Council that is it not done via a non-EEA route ***Need system info to be definite but understanding is that data will be transferred by a physical cable.***	
12. Exemptions				
12.1	Will any exemptions for specific types of processing be relied on? E.g. crime prevention, regulatory purposes.	Prevention of crime. Evidence gathering for potential legal and/or enforcement action. Refer to 2.1		

Overall Compliance Summary	

	Electronic Signature	Title	Date of PIA	Completion Date
Project Manager				
Data Protection Officer				

Copy to be retained by the Project Manager with the project documentation. Copy to be retained by the Data Protection Officer.