SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

CITY OF WOLVERHAMPTON COUNCIL

Data Protection Impact Assessment

Taxi CCTV Policy

Project name: Taxi CCTV Policy

Data controller: Vehicle Licence Holders

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☐ Targeting children / vulnerable adults
☐ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

Whilst City of Wolverhampton Council is not the Data Controller, a DPIA has been undertaken as a precautionary measure. Licence holders should also undertake a DPIA.

2. What are the timescales and status of your surveillance camera deployment?

This is the proposal for a policy on the voluntary installation of surveillance cameras within licensed vehicles by the vehicle proprietor. If the policy is approved, installation could begin in April 2021.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

In 2019 there were 302 crimes recorded by West Midlands Police that involved licensed vehicles in Wolverhampton. The Hackney Carriage and Private Hire trades have raised the issues of violence and theft against drivers in meetings of the trade working group.

Licensing Services already encourages self-reporting of incidents by passengers and drivers, with all complaints investigated. Surveillance camera footage will assist in making accurate and fair licensing decisions. There have been several occasions when investigating complaints where surveillance camera footage would have assisted, due to conflicting accounts.

CCTV cameras can help deter crime, but also provide evidence of crimes which can be used by the police to apprehend perpetrators and used in court to achieve succcesul prosections.

The deterrance of crime is the primary objective of this project, particularly to safeguard vulnerable passengers and reassure drivers.

The Department for Transport's 'Statutory taxi and private hire vehicle standards' recommended consulting on CCTV. The ICO and Surveillance Commissioner have given the

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

strongest possible advice that mandatory CCTV is very difficult for licensing authorities to justify.

The outcome of the Council's consultation on CCTV in taxis indicated that a mandatory requirement for CCTV would not be proportionate. As such, CCTV is not required by Licensing Services, however a policy is proposed to outline the requirements for those wishing to voluntarily install CCTV.

4. Whose personal data will you be processing, and over what area?

The system will be able to record internal video footage of the driver and any passengers in the vehicle when the vehicle is being used as for private hire or hackney carriage use. Passengers can be anybody, including children or vulnerable groups.

Where external facing cameras are installed, other vehicles including number plates will be captured, along with images of pedestrians.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved?

The Data Controller is the vehicle licence holder. It is likely that the police will request data to assist with their investigations as well as Licensing Services.

The licence holder must comply with valid information requests, in consideration of The Data Protection Act (2018) and General Data Protection Regulations (GDPR). Data must be shared securely and requests must be fulfilled without charge. Data must only be shared for the following reasons:

a) where a crime report has been made involving the specific vehicle and the Police have formally requested that data.
b) when a substantive complaint has been made to the licensing authority regarding a specific vehicle / driver and that complaint is evidenced in writing (and cannot be resolved in any other way).
c) where a Data request is received from an applicant e.g. police or social services, that has a legal basis to have access to the data requested to assist them in an investigation that involves a licensed vehicle or driver.
d) Subject Access Request compliant with the GDPR. The DPA gives individuals the right to see information held about them, including CCTV images of them.

Each data request must be considered on its own merits by the Data Controller and whether it would be lawful.

6. How is information collected? (tick multiple options if necessary)

- ☐ Fixed CCTV (networked)
- ☐ Body Worn Video
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Redeployable CCTV
- ☒ Other (please specify)

The licence holder will choose which system to install, dependent on their requirements and its suitability.

City of Wolverhampton Council cannot justify audio recording within its licensed vehicles. As such, CCTV systems must not be used to record conversations as this is highly intrusive to people's data rights and unjustified in meeting the purpose of preventing and evidencing crimes

Licence holders should choose a system without this facility where possible and any system that comes equipped with an independent sound recording facility must be turned off or disabled in some other way.

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram.

CCTV records footage onto a secure storage format. Footage is retained for maximum 31 days and then overwritten or deleted. Where a valid information request is received by the data controller, they can share the relevant footage. This footage must then be deleted at the earliest appropriate opportunity following conclusion of the request.

8. Does the system's technology enable recording?

- ☒ Yes
- ☐ No

In-vehicle surveillance camera, recorded to onboard encrypted storage system.

9. If data is being disclosed, how will this be done?

- ☐ Only by on-site visiting
- ☐ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)
- ☐ Off-site from remote server
- ☒ Other (please specify)

When the Data Controller shares data as the result of a lawful request, this must be via a secure method as outlined in the policy, such as:

- Secure email
- Encrypted email
- Encrypted data drive
- Encrypted Disc, transferred directly or via a secure courrier/mailing service.

- Secure online storage/ file transfer

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☐ Used to search for vulnerable persons

☐ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☒ Recorded data disclosed to authorised agencies to provide intelligence

☐ Other (please specify)

Consultation

Stakeholder consulted	Consultation method	Views raised	Measures taken
Black Country Chamber of Commerce	Online consultation	Awaiting response	TBC
City of Wolverhampton Council - Councillors	Online consultation	Awaiting response	TBC
City of Wolverhampton Council – Equalities	Online consultation	Awaiting response	TBC
City of Wolverhampton Council - ICT	Online consultation	Awaiting response	TBC
City of Wolverhampton Council - Information Governance	Online consultation	Awaiting response	TBC
City of Wolverhampton Council – Legal Services	Online consultation	Awaiting response	TBC
City of Wolverhampton Council – Licensing Services	Online consultation	Awaiting response	TBC
City of Wolverhampton Council – School Transport	Online consultation	Awaiting response	TBC
City of Wolverhampton Councillors	Online consultation	Awaiting response	TBC
Department for Transport	Online consultation	Awaiting response	TBC
Information Commissioner	Online consultation	Awaiting response	TBC
Pubwatch	Online consultation	Awaiting response	TBC
Surveillance Camera Commissioner	Online consultation	Awaiting response	TBC
City of Wolverhampton Council private hire and hackney carriage licence holders	Online consultation	Awaiting response	TBC
The public, as customers of the trade	Online consultation	Awaiting response	TBC
Transport for West Midlands	Online consultation	Awaiting response	TBC
West Midlands Police	Online consultation	Awaiting response	TBC
Wolverhampton's Multi-Agency Safeguarding Hub (MASH)	Online consultation	Awaiting response	TBC

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system?

Local Authorities

For the processing of personal data GDPR Article 6 1(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;

The basis for the processing referred to in point (e) of shall be laid down by:

1. Union law; or

2. Member State law to which the controller is subject.

The relevant law is: Local Government (Miscellaneous Provisions) Act 1976 Part II Section 51. This contains the statement "(2)A district council may attach to the grant of a licence under this section such conditions as they may consider reasonably necessary.

Section 111 Local Government Act and Section 1 Localism Act provide the legal powers which allow the Council to undertake the above.

For the processing of special category data GDPR Article 9 1(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

The function is conferred on a person by an enactment or is of a public nature and is exercised in the public interest.

Licensing is a **function that is designed to protect the public** against **unfitness or incompetence** and **is of a public nature** and is **exercised in the public interest** to **protect persons other than those at work** (i.e. the public) **against risk to health or safety arising out of or in connection with the action of persons at work** (i.e. a private hire/hackney carriage driver).

This information will be recorded in the interests of public safety, crime detection and crime prevention.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information?

Any vehicle fitted with CCTV must display clearly visible and readable signage informing passengers that such a system is fitted. This signage must be displayed so as to minimise obstruction but must be visible before and after entering the vehicle.

The signage must contain:

- The purpose for using the surveillance system, "in the interests of public safety, crime detection and crime prevention".
- The name and contact number of the Data Controller, which should be the vehicle licence holder. **City of Wolverhampton Council's is not the Data Controller.**

If signage is lost or removed, new signage must be installed prior to any licensable activities being undertaken.

The driver should verbally advise that CCTV is in operation where necessary e.g. where people may have visual impairments and/or hearing difficulties.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes?

Audio recording is prohibited and breaches of the Taxi CCTV Policy will result in enforcement action against the licence holder.

The licence holder will be the Data Controller.

The licence holder must comply with valid information requests, in consideration of The Data Protection Act (2018) and General Data Protection Regulations (GDPR). Data must be shared securely and requests must be fulfilled without charge. Data must only be shared where there is a valid lawful reason, such as;

a) where a crime report has been made involving the specific vehicle and the Police have formally requested that data.
b) when a substantive complaint has been made to the licensing authority regarding a specific vehicle / driver and that complaint is evidenced in writing (and cannot be resolved in any other way).
c) where a Data request is received from an applicant e.g. police or social services, that has a legal basis to have access to the data requested to assist them in an investigation that involves a licensed vehicle or driver.
d) Subject Access Request compliant with the GDPR. The DPA gives individuals the right to see information held about them, including CCTV images of them.

This list is not exhaustive, and it is the responsibility of the Data Controller to consider the lawfulness of requests to share information in line with UK Data Protection Law.

The uploading of footage to social media does not have a lawful basis, is not legitimate sharing and, it is expressly prohibited. This includes, by way of examples, but is not limited to: YouTube, WhatsApp, Instagram, TikTok, Facebook and Twitter. Where licence holders' have shared footage unlawfully, they will be liable to criminal prosecution. Unlawful sharing is a breach of UK Data Protection Law and is considered a breach of policy. Breaches of policy are dealt with by way of reviewing a vehicle licence.

15. How long is data stored? (please state and explain the retention period)

31 days or until the outcome of a legitimate and lawful request.

16. Retention Procedure

☒ Data automatically deleted after retention period

☒ System operator required to initiate deletion

☒ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

Data stored in the encrypted onboard storage should be automatically deleted after 31 days. Data shared must be deleted by the recipient after it is no longer lawfully necessay for it to be retained.

17. How will you ensure the security and integrity of the data?

See risk assessment overleaf.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information?

The Data Controller is required to comply with these requests.

19. What other less intrusive solutions have been considered?

Self-reporting is encouraged of incidents by drivers and passengers. Some drivers use app-based software, which offers safety features for passengers such as distress signals, journey display

20. Is there a written policy specifying the following?

☒ The agencies that are granted access

☒ How information is disclosed

☒ How information is handled

Are these procedures made public? ☒ Yes ☐ No

Once approved, the Taxi CCTV Policy will be published online.

Are there auditing mechanisms? ☐ Yes ☒ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

Identify and address the risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved?**
Risk that the CCTV systems are used inappropriately/ incorrectly	Possible	Significant	Medium	All licence holders are required to undergo a 'fit and proper' test. Breaches of the Taxi CCTV Policy would result in the review of their licence.	Reduced	Low	Awaiting consultation feedback
Capturing excessive data	Probable	Significant	Medium	The policy informs people of their legal responsibilities and acts as a deterrent from breaking the law and policy. It is stated that audio recording is prohibited and that Data Controllers should choose a system without this facility where possible. Where the system comes equipped with an independent sound recording facility, it must be turned off or disabled in some other way.	Reduced	Low	Awaiting consultation feedback
Vehicle occupants uninformed that they are being recorded.	Probable	Minimal	Low	A six-week public consultation on surveillance cameras in licensed vehicles.	Reduced	High	Yes
				Signage advising of the surveillance cameras to be clearly visible from all seats.	Reduced	Low	Awaiting consultation feedback

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved?**
				An audio warning plays when the vehicle is being used for a licensable activity. The warning shall include that surveillance cameras are recording video throughout the journey, but audio recording will only begin if a panic button is pressed or someone shouts in the vehicle.	Reduced	Low	Awaiting consultation feedback
Unauthorised access to data	Possible	Severe	High	System must store data securely and the Data Controller may only share data when a lawful request is received.	Reduced	Medium	Awaiting consultation feedback
				Transfer of data must be done securely.	Reduced	Low	Awaiting consultation feedback
				Data recorded by the system must not be displayed on digital screens in the vehicle.	Reduced	Low	Awaiting consultation feedback
				Where licence holders' have shared footage unlawfully, they will be liable to criminal prosecution. Unlawful sharing is a breach of UK Data	Reduced	Low	Awaiting consultation feedback

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved?**
				Protection law and is considered a breach of policy. This is recorded in the policy and informing people they are criminally and financially liable for any misuse may deter people from doing so.			
				Data must only be transferred following a legitimate and lawful data request.	Reduced	Medium	Yes

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. Further information is on the ICO website.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

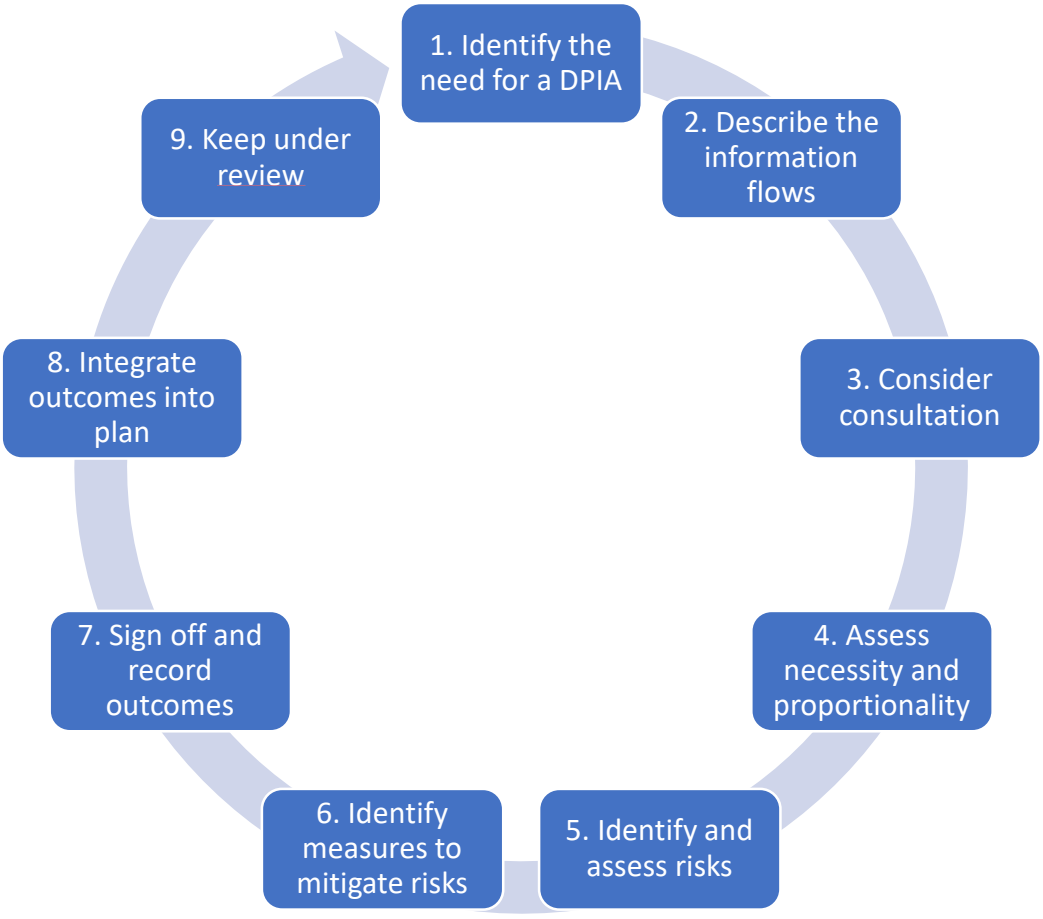
APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Vehicle interior, with driver and all passengers in view		1-9 per vehicle	31 days	When the vehicle is in use.	Cameras are installed here to be a visible deterrent and to record the behaviour of the individuals in the field of view.

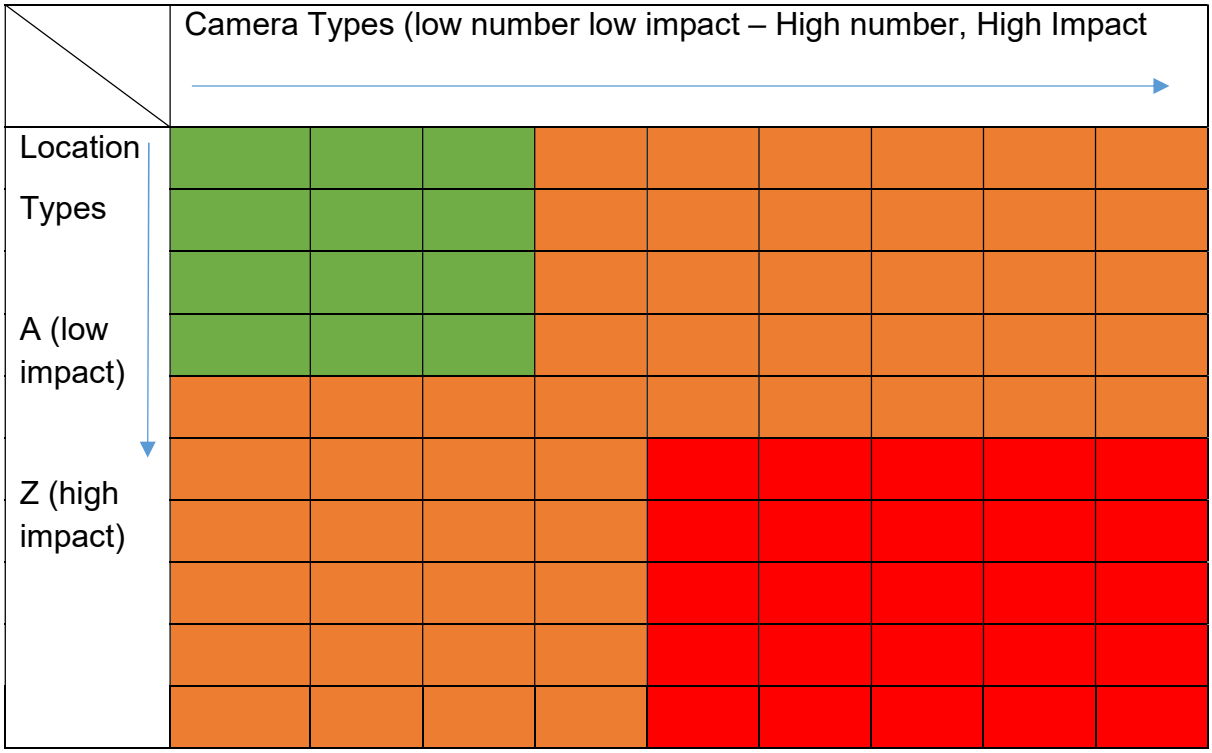
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:



NOTES