



**SURVEILLANCE CAMERA
COMMISSIONER**



**CITY OF
WOLVERHAMPTON
C O U N C I L**

Data Protection Impact Assessment

**Surveillance Cameras in Vehicles
Licensed for use as a Private Hire or
Hackney Carriage**



Project name: Surveillance Cameras in Vehicles Licensed for use as a Private Hire or Hackney Carriage

Data controller: City of Wolverhampton Council

1. Identify why your deployment of surveillance cameras requires a DPIA¹:

- | | |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input checked="" type="checkbox"/> Large scale use of sensitive data |
| <input checked="" type="checkbox"/> Public monitoring | <input checked="" type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input checked="" type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input type="checkbox"/> Other (please specify) |

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

This is the proposal for a new surveillance camera system within licensed vehicles. If a system is approved, installation could begin in 2021.

The system will be GDPR compliant.

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.

Surveillance 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 successful prosecutions.

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

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

The system will 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.

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/>

When the vehicle is being used for personal use, the system will only record external video footage.

Audio recording is not normally recorded, but a five minute recording will be triggered by:

- Passengers' panic button
- Driver's panic button
- G-force sensor indicating a crash
- Shouting detected by a microphone
- Door opening when vehicle is in motion

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

Licensing Services will be the primary user of the data, however it is likely that the police will request data to assist with their investigations as well.

Other requests are expected from:

- Other licensing authorities – to make a licensing decision on a licensed driver or vehicle proprietor
- Motor insurance companies – to investigate claims made by the driver, vehicle proprietor or other drivers involved in an accident with the vehicle

When data is shared this is normally via:

- Secure email
- Encrypted email
- Encrypted data drive
- Disc, transferred directly between officers from the organisations
- Secure online storage

Each data request will be considered on its own merits and whether it would be lawful.

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

- | | |
|--|---|
| <input type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Redeployable CCTV |
| <input checked="" type="checkbox"/> Other (please specify) | |

Multiple cameras will be located in the vehicle, with recording capability of all passengers and the driver. These cameras will be connected to a recording unit within the vehicle.

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

See file 'Surveillance Camera Information Flow'.

8. Does the system's technology enable recording?

- Yes No

In-vehicle surveillance camera, recorded to onboard encrypted storage system. Further detail in Section 4.

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)

Footage will be retrieved by an authorised officer in the course of investigating a complaint or crime. Depending on the solution procured, this may be via physical or remote connection.

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)

The surveillance cameras will provide video and audio data, which will be recorded by the system along with the vehicle's location (calculated using the Global Positioning System) and g-force data. This will provide the vehicle's location, speed and if there has been a collision.

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?

Schedule 2, Part 2 (7) of the Data Protection Act 2018 states that the listed GDPR provisions [in Schedule 2 Part 2 (6)] do not apply to personal data processed for the purpose of discharging a function that is designed to protect the public - to the extent that the application of those provisions would be likely to prejudice the proper discharge of that function.

Schedule 2 Part 2 (7) (2) applies where the function is designed to protect members of the public against:

(a) dishonesty, malpractice or other seriously improper conduct

or

(b) unfitness or incompetence

and

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

Schedule 2 Part 2 (7) (4) applies where the function is designed:

(a) to secure the health, safety and welfare of persons at work

or

(b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work

and

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 and to enable the Council to discharge its statutory licensing functions as required by Local Government (Miscellaneous Provisions) Act 1976 Part II Section 51.

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

Surveillance cameras are part of the UK's transport network, including trains, buses and taxis licensed by other authorities. Data subjects could reasonably expect to be recorded by a surveillance camera in a taxi.

Signage provided by City of Wolverhampton Council informing of the surveillance camera must be displayed prominently in the vehicle. If signage is lost or removed, new signage must be obtained from the council at the earliest opportunity and prior to any further licensable activities being undertaken.

CCTV in operation



This vehicle is protected by CCTV in the interests of public safety, crime detection and crime prevention.

Audio recording may also be made in the event of an incident.

The CCTV has been installed in accordance with the Surveillance Camera policy of City of Wolverhampton Council.

CITY OF
WOLVERHAMPTON
COUNCIL

For more information:

01902 55 TAXI

www.wolverhampton.gov.uk

An audio message will play after a vehicle's door closes when the vehicle is in use as a private hire or hackney carriage vehicle.

The system will operate in compliance with City of Wolverhampton Council's Privacy Notice: <https://www.wolverhampton.gov.uk/your-council/our-website/privacy-and-cookies-notice>

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

Data is only recorded when reasonable to strike a balance of deterring crime whilst protecting passenger and driver privacy. Licensing Services should see an increase of investigations where footage can be used to inform the outcome.

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

31 days on the onboard system, otherwise until the legitimate transfer as the result of a legitimate and lawful request, or the outcome of the council's investigation a complaint and any subsequent legal appeals process.

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 will be automatically deleted after 31 days. Data retrieved by an authorised officer will be deleted after the appeals process has been concluded after the licensing decision has been made, or after it has been transferred to the police.

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?

In accordance with the Council's current Privacy Notice and data request procedures.

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

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)

The Council's internal Audit and Information Governance services govern Licensing Services' information sharing processes.

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?
Passenger and driver safety	Probable	Significant	Medium	Whilst data recording is not in operation, the system displays a warning that the vehicle is not currently licensed for use as a private hire or hackney carriage vehicle. The system begins recording following an input from the driver's licence and the system displays a message that the vehicle is available for use as a licensed vehicle.	Reduced	Low	Awaiting consultation feedback
				Data recording continues for five minutes after a change in vehicle voltage and only stops if there has been five consecutive minutes with a low vehicle voltage (indicating that the ignition is not on).	Reduced	Low	Awaiting consultation feedback
				If the camera view is obstructed, the system will display a warning message.	Reduced	Medium	Awaiting consultation feedback

Passenger and driver privacy	Probable	Significant	Medium	<p>Audio recording is disabled by default, but a five-minute recording is triggered by:</p> <ul style="list-style-type: none"> • Passengers' panic button • Driver's panic button • G-force sensor indicating a crash (>4 g) • Shouting detected by a microphone • Door opening when vehicle is in motion <p>An audible warning and visual light shall indicate when audio recording is occurring.</p>	Reduced	Low	Awaiting consultation feedback
Driver's privacy	Probable	Minimal	Low	Data recording does not take place until it is triggered by the presence of a driver licence, to indicate that the driver wants to use the vehicle for a licensable activity.	Eliminated	Low	Awaiting consultation feedback
Vehicle occupants uninformed that they are being recorded.	Probable	Minimal	Low	A twelve-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
				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	Reduced	Low	Awaiting consultation feedback

				begin if a panic button is pressed or someone shouts in the vehicle.			
Unauthorised access to data	Possible	Severe	High	System must have security features which protect against tampering and indicate if the system has been tampered with.	Reduced	Medium	Awaiting consultation feedback
				Transfer of data will be done securely, in accordance with the council's data transfer processes.	Reduced	Low	Awaiting consultation feedback
				Stored data encrypted to 128-bit Advanced Encryption Standard equivalent or higher.	Reduced	Low	Awaiting consultation feedback
				Data recorded by the system will only be accessible by authorised officers and will not be displayed in the vehicle.	Reduced	Low	Awaiting consultation feedback
				Data will only be transferred outside of City of Wolverhampton Council following a legitimate and lawful written data request.	Reduced	Medium	Yes
				The system will log the following actions, accompanied by the actioning account name, time and date: <ul style="list-style-type: none"> • each user access • camera system parameter modifications 	Reduced	Medium	Awaiting consultation feedback

				<ul style="list-style-type: none"> • each image download session • modification/manipulation of downloaded images • exporting of downloaded images exporting of downloaded clips			
Unauthorised or accidental destruction of data	Possible	Significant	High	100% solid state design or a proven vibration and shock resistant system. The system should not have a cooling fan and the recording should be vibration and shock proof.	Reduced	Low	Awaiting consultation feedback
				Flash-based SSD (100% industrial grade).	Reduced	Low	Awaiting consultation feedback
				Hard disk with both mechanical anti-vibration and anti-shock mechanism and self-recovery and self-check file writing system.	Reduced	Low	Awaiting consultation feedback
				System to be protected against reverse voltage.	Reduced	High	Awaiting consultation feedback
				System to be protected against high voltage transients likely to be encountered in the vehicle electrical system.	Reduced	High	Awaiting consultation feedback

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)
Public car park	1, 5, 6	100			
Vehicle interior, with driver and all passengers in view		≤3 per vehicle	31 days	After the driver triggers the system with their driver licence, until 5 minutes after a drop in vehicle voltage indicating engine is off.	High-definition cameras are installed here to be a visible deterrent and to record the behaviour of the individuals in the field of view.
Front and rear windscreen, facing outside		2	31 days	After a change in vehicle voltage to indicate that the engine is on, until 5 minutes after a drop in vehicle voltage indicating engine is off.	High-definition cameras are installed here to record the driver's driving and any road traffic accidents.

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:

	Camera Types (low number low impact – High number, High Impact)								
	→								
Location	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange
Types	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange
A (low impact)	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange
Z (high impact)	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red

NOTES