

Taxi CCTV Policy

Licensing Services

Created: 12 October 2020

Revised: 3 June 2026

Contents

Scope.....	2
Purpose.....	2
Legality.....	3
Compliance, Regulation and Complaints	3
ICO Registration as Data Controller.....	3
Data Processors.....	4
Audio Recording.....	4
Signage and Advising of Cameras	5
Storage of Data	5
Sharing Data	5
Summary of CCTV and Dashcam Requirements	6

Scope

City of Wolverhampton Council licensed Hackney Carriages and Private Hire Vehicles are referred to collectively as 'licensed vehicles' in this policy. These are commonly referred to as taxis.

This policy relates to in-vehicle cameras, also known as surveillance cameras, in licensed vehicles:

For the purposes of this policy, there are two types of cameras permitted:

1. External facing dashcams, that do not record audio.
2. Closed Circuit Television (CCTV), from the Council's [approved list](#), which records audio when a panic-switch is activated.

Both types of systems require registration with the Information Commissioner's Office.

Passengers must not be visible on any footage recorded by dashcams and audio recording on dashcams is strictly prohibited. An inward facing dashcam is not authorised CCTV.

Proprietors of vehicles licensed by City of Wolverhampton Council are permitted to voluntarily install in-vehicle cameras, subject to adherence with this policy throughout the duration of the proprietor's licence.

Licence holders are advised that school transport contracts may preclude the installation of CCTV in their vehicle and that they should engage with their contract manager prior to purchasing a CCTV system.

Purpose

The policy's purpose is to facilitate the use of in-vehicle cameras in licensed vehicles, to protect drivers and passengers, whilst ensuring licence holders respect passenger privacy.

This protection is intended to come from:

- Visible surveillance cameras deterring individuals from committing a crime through the knowledge that evidence of it will be recorded.
- Occupants of the vehicle feeling reassured that crimes, as well as malicious complaints against drivers, are less likely to occur in an environment protected by in-vehicle cameras.
- Informing investigations by the Council and police.

This policy does not require in-vehicle cameras to be in operation. However, if the driver of the vehicle is not the owner of the vehicle, they should check with the vehicle licence holder under what circumstances they are permitted to disable recording, in accordance with their operating procedures and risk assessment.

The absence of in-vehicle cameras in a licensed vehicle does not indicate that the owner of the vehicle has failed to pay attention to passenger or driver safety and their 'fitness and propriety' is not in question.

Legality

Data recorded by any CCTV system must be handled in accordance with The Data Protection Act and UK GDPR. The Information Commissioner's Office (ICO) is the UK regulator for all matters relating to the use of personal data.

It is contrary to the Motor Vehicle (Construction and Use) Regulations 1986, for equipment to obscure the driver's view of the road through the windscreen.

Compliance, Regulation and Complaints

The Surveillance Camera Commissioner (SCC) works to encourage compliance with the '[Surveillance camera code of practice](#)'.

The Information Commissioner's Office (ICO) is the regulatory body responsible for enforcing compliance with privacy and data protection legislation.

Licence holders must comply with any relevant guidance issued by the SCC and ICO.

If a passenger or any other individual wants to request footage relating to themselves, they should make a Subject Access Request (SAR) to the Data Controller detailed on the signage in the vehicle. Signage is covered in greater detail in this document, under the section 'Signage and Advising of Cameras'. Information on how to make a valid SAR is available at <https://ico.org.uk/for-the-public/make-a-subject-access-request/>

If a passenger has an issue with their journey relating to the footage recorded, they should contact the Data Controller in the first instance, using the details displayed on the signage within the vehicle.

If the Data Controller fails to resolve the issue, the complainant may escalate this to the ICO at <https://ico.org.uk/make-a-complaint/>

ICO Registration as Data Controller

The ICO defines a 'Data Controller' as the individual or organisation which has ultimate responsibility for how personal data is collected and processed.

For the purpose of the installation and operation of in-vehicle cameras, the Data Controller is the vehicle licence holder. The licence holder must be registered with the [Information Commissioner's Office](#) and be able to evidence continuous registration throughout the lifetime of the licence.

Registration with the Information Commissioner's Office requires renewal on an annual basis and payment of the appropriate fee.

Individuals can request to have their address removed from the public register. Individuals can contact the Information Commissioners Officer registration team on 0303 123 1113 to make a request their home address is removed from the entry on the public register.

Data Processors

A Data Processor, in relation to personal data, means any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller, in response to specific instructions. Where a service provider is authorised for the remote storage and/or management of data, they will act as a 'Data Processor'.

There must be a formal written contract between the Data Controller and Data Processor. The contract must contain provisions covering security arrangements, retention/deletion instructions, access requests and termination arrangements.

Audio Recording

If the proprietor wants to install a system which has panic-switch activated audio recording facilities compliant with the requirements of this section, it must be installed by a professional supplier. The requirements are as follows:

- The system must not record audio, unless activated by a switch supplied by the manufacturer and installed professionally. The switch must be accessible to both the driver and passengers.
- The switch must then provide an illuminated visual indicator, clearly visible from all passenger seats, that audio recording is taking place. The driver must verbally inform the passengers that audio is recording.
- Once activated, the audio recording must be synchronised to the CCTV video recording and embedded within the same data file. This file must be protected against tampering.
- If the engine is turned off, audio recording must continue for at least 10 minutes.
- Audio recording must cease within 1 minute of the switch being deactivated.

Approved systems and suppliers are available at www.wolverhampton.gov.uk/licences/licensed_vehicle-licences/ApprovedCCTV

The supplier must provide the certificate of installation and the registration plate of the vehicle, for this to be linked to the vehicle's record.

Vehicles equipped with an audio recording CCTV system must obtain the appropriate warning signage from the council.

Failure to arrange for these documents to be provided to Licensing Services will be considered misconduct, even if the system complies with the other policy

requirements, resulting in a review of relevant licences.

Signage and Advising of Cameras

Any vehicle fitted with CCTV or dashcams 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. At a minimum, this will be a double-sided sticker in the window on the left and right sides of 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 is not the Data Controller.**
- The Data Controller’s ICO Registration Number.

Signage is available from Licensing Services. 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 or where they have been informed in advance that the booked passenger has a disability.

Storage of Data

Data must be handled securely in a way that ‘ensures appropriate security’, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. CCTV footage must be encrypted to prevent unauthorised access, with appropriate controls to limit access to relevant individuals only, such as password protection. Data should be deleted after 31 days, unless it has been legitimately shared, in which case it should be deleted when appropriate on the conclusion of the request.

Digital screens within the vehicle for the purposes of viewing footage are prohibited.

Sharing Data

The licence holder must comply with valid information requests, in consideration of The Data Protection Act (2018) and UK General Data Protection Regulations (UK 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, for example:

- 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) a Subject Access Request (SAR) compliant with the UK GDPR. The DPA gives individuals the right to see information held about them, including CCTV images of them. More information on the Data Controller's responsibilities relating to SARs is available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/>

This list is not exhaustive; 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 CCTV and dashcam footage to social media does not have a lawful basis 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, as it violates the privacy rights of the individuals recorded – even if it is footage which shows a passenger behaving badly or of another driver driving dangerously. These data subjects may complain to the Information Commissioner's Office (ICO), which may result in a fine for you. In addition, the publication of this footage may compromise legal proceedings.

If you have dashcam footage of a suspected driving offence, you can report this to your police force. Search 'Operation Snap' online.

Summary of CCTV and Dashcam Requirements

1. Licence holders must comply with any relevant guidance issued by the Surveillance Camera Commissioner and Information Commissioner's Office.
2. The vehicle proprietor must be registered with the [Information Commissioner's Office](#) and be able to evidence continuous registration throughout the lifetime of the licence.
3. Clearly visible and readable signage advising of the system and the Data Controller's contact details, including ICO registration number, must be displayed in the vehicle.
4. The system must not obscure the driver's view of the road through the windscreen.
5. The system may only record audio in line with the requirements of Audio Recording on page 4.
6. Data must be stored securely, with access controls to prevent unauthorised access and only shared when lawful.

A vehicle licence may be refused, suspended or revoked where the camera system does not comply with this policy, or on any other reasonable grounds. The driver's licence may also be reviewed.