Policy regarding CCTV systems in Leicester City Council licensed vehicles

Leicester City Council

Contents

Introduction

These guidelines set out to ensure that CCTV systems voluntarily installed in Hackney Carriages (HCV's) and Private Hire Vehicles (PHVs) licensed by Leicester City Council are properly managed whilst being used to prevent and detect crime; and enhance the health, safety and security of both Hackney/PHV drivers and passengers.

Vehicle owners, who may also be the driver and/or operator, installing CCTV systems must fully comply with the requirements set out in these guidelines.
For the purposes of these guidelines the term "CCTV system" will include any electronic recording device attached to the inside of vehicle having the technical capability of capturing and retaining visual images from inside or external to the vehicle. In addition to the standard CCTV camera system these may include for example, such devices as events/incident/accident data recording devices.

The purpose of CCTV

The purpose of the CCTV system shall be to provide a safer environment for the benefit of the Hackney/PHV driver and passengers by:

- Deterring and preventing the occurrence of crime
- Reducing the fear of crime
- Assisting the Police/Licensing Authority in investigating incidents of crime/breaches
- Assisting insurance companies in investigating motor vehicle accidents

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 CCTV footage relating to themself, 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 CCTV'. Information on how to make a valid SAR is available at https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

If a passenger has an issue with their taxi journey relating to the use of CCTV they should contact the Data Controller, in the first instance, using the details displayed on the CCTV 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 CCTV, 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.

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 CCTV 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

Leicester City Council cannot justify audio recording within its licensed vehicles as a proportionate solution to prevent and record crime. 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. You should choose a system without this facility where possible and any system with an independent sound recording facility must have audio recording turned off or disabled in some other way.

Signage and Advising of CCTV

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. 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. (Leicester City Council is **not** the Data Controller)
- The Data Controller's ICO Registration Number.

Signage will be available to purchase 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.

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/licensing authority, 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/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

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 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.

Summary of CCTV 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 must not record audio at any time.
6. The system must be recording on **any** journey the vehicle is used for taxi purposes if fitted.
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 CCTV system does not comply with this policy, or on any other reasonable grounds.