**APPENDIX E**

## CCTV IN VEHICLES

Caerphilly County Borough Council Licensing recognises that an in-vehicle CCTV system may provide a safer environment for the benefit of the drivers and passengers by deterring and preventing the occurrence of crime; reducing the fear of crime; assisting the Police in investigating incidents of crime. As such CCBC permits the use of CCTV in private hire / hackney carriage vehicles subject to compliance with the best practice guidance set out below.

## BEST PRACTICE GUIDANCE - CCTV SYSTEMS IN LICENSED HACKNEY CARRIAGE AND PRIVATE HIRE VEHICLES

### Introduction

This guidance sets out to ensure that in-vehicle CCTV systems in licensed vehicles are used to prevent and detect crime, reduce the fear of crime and enhance the health and safety of drivers and passengers alike.
Vehicle owners, who may also be the driver and/or operator, installing in-vehicle CCTV systems should fully comply with the requirements set out in these guidelines.
The purpose of the in-vehicle CCTV system shall be to provide a safer environment for the benefit of the drivers and passengers by:

- Deterring and preventing the occurrence of crime;
- Reducing the fear of crime;
- Assisting the Police in investigating incidents of crime.

### General Requirements

Any in-vehicle CCTV system to be fitted should, as a minimum, meet the requirements set out in this guidance. Only in-vehicle CCTV systems meeting these requirements should be installed into licensed vehicles.

The installation and operation of in-vehicle CCTV must comply with the requirements of the Information Commissioner's CCTV Code of Practice, which is available via the following link:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

All equipment must comply with any legislative requirements in respect of Motor Vehicle Construction and Use Regulations.

All equipment must meet all requirements as regards safety, technical acceptability and operational/date integrity.

All equipment must be designed, constructed and installed in such a way and in such materials as to present no danger to passengers or driver, including impact with the equipment in the event of a collision or danger from the electrical integrity being breached through vandalism, misuse, or wear and tear.

**Automotive Electromagnetic Compatibility Requirements (EMC)**

CCTV equipment must not interfere with any other safety, control, electrical, computer, navigation, satellite, or radio system in the vehicle.
Any electrical equipment such as in-vehicle CCTV system fitted after the vehicle has been manufactured and registered, is deemed to be an Electronic Sub Assembly (ESA) under the European Community Automotive Electromagnetic Compatibility Directive and there must meet with requirements specified in that Directive.

CCTV equipment should be e-marked or CE-marked and be confirmed by the equipment manufacturer as being suitable for use in motor vehicles.

**Camera Design Requirements**

The camera must be fitted safely and securely, should not adversely encroach the passenger area and must not impact on the safety of the driver, passenger or other road users.

The installed in-vehicle CCTV system must not weaken the structure or any component part of the vehicle or interfere with the integrity of the manufacturer's original equipment.

All equipment must be installed in such a manner so as not to increase the risk of injury and/or discomfort to the driver and/or passengers. The camera must be attached by means of a permanent method; i.e. screw fixings or a specifically designed permanent adhesive pad supplied by the CCTV system supplier (pads similar to those used by car manufacturers for the attachment of interior mirrors).

All equipment must be protected from the elements, secure from tampering and located such as to have the minimum intrusion into any passenger area or impact on the luggage carrying capacity of the vehicle.

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

Equipment must not obscure or interfere with the operation of any of the vehicle's standard and/or mandatory equipment, i.e. not mounted on or adjacent to air bags or within proximity of other supplementary safety systems which may cause degradation in performance or functionality of such safety systems.

Viewing screens within the vehicle for the purposes of viewing captured images will not be permitted.

All wiring must be fused as set out in the manufacture's technical specification and be appropriately routed.

All equipment must be checked regularly and maintained to operational standards, including any repairs after damage.

All system components requiring calibration in situ should be easily accessible.

**Camera Activation Methods**

Activation of the equipment may be via a number and combination of options, such as – door switches, time delay and drivers' panic button. A direct wired link to the vehicles taximeter, in the case of a Taxi, will not be acceptable.
Audio Recording
In-vehicle CCTV systems must not be used to record conversations between members of the public as this is highly intrusive.

**Image Security**

Images captured must remain secure at all times.

The captured images must be protected using approved encryption software which is designed to guard against the compromise of the stored data, for example, in the event of the vehicle or equipment being stolen. It is recommended by the Information Commissioner's Office (ICO) that "data controllers" ensure any encryption software used meets or exceeds the current FIPS 140-2 standard or equivalent. System protection access codes will also be required to ensure permanent security.

**Retention of CCTV images**

The in-vehicle CCTV equipment selected for installation must have the capacity of retaining images either:-

- Within its own hard drive;
- Using a fully secured and appropriately encrypted detachable mass storage device, for example, a compact flash solid state card;
- Or where a service provider is providing storage facilities, transferred in real time using fully secured and appropriately encrypted GPRS (GSM telephone) signalling to a secure server within the service provider's monitoring centre.

Images must not be downloaded onto any kind of portable media device (e.g. CDs or memory sticks) for the purpose of general storage outside the vehicle.

In-vehicle CCTV equipment selected for installation must include an automatic overwriting function, so that images are only retained within the installed system storage device for a maximum period of 31 days from the date of capture. Where a service provider is used to store images on a secure server, the specified retention period must also only be for a maximum period of 31 days from the date of capture.

**Notification to the Information Commissioner's Office**

The Information Commissioner's Office (ICO) is the official regulator for all matters relating to the use of personal data.

The ICO defines a "data controller" as the body which has legal responsibility under the Data Protection Act (DPA) 1998 for all matters concerning the use of personal

data. For the purpose of the installation and operation of in-vehicle CCTV, the "data controller" is the specified company, organisation or individual which has decided to have in-vehicle CCTV installed. The data controller has the final decision on how the images are stored and used and determines in what circumstances the images should be disclosed.

Notification is the process by which a data controller informs the ICO of certain details about their processing of personal information. These details are used to make an entry in the public register of data controllers.This means that any specified company, organisation or individual vehicle owner who has a CCTV system installed in a licensed vehicle must register with the ICO (Notification) and obtain documented evidence of that registration. This documentary evidence may be required to be presented to an authorised officer at any time during the term of the vehicle licence. The Notification requires renewal on an annual basis, and payment of the appropriate fee.

**Using a third party service provider (data processor)**

Where a service provider is used for the remote storage of CCTV data they will act as a "data processor".

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. The data controller retains full responsibility for the actions of the data processor.

There must be a formal written contract between the data controller and data processor (service provider). The contract must contain provisions covering security arrangements, retention/deletion instructions, access requests and termination arrangements.

Documentary evidence of the contractual arrangements may be required to be presented to an authorised officer at any time during the term of the vehicle licence.
Use of information recorded using in-vehicle CCTV

The data controller is responsible for complying with all relevant data protection legislation. The data controller is legally responsible for the use of all images including breaches of legislation.

Any images should only be used for the purposes described earlier in these guidelines.

Requests may be made by the Police or other law enforcement agencies, an authorised officer or exceptionally other appropriate bodies to the "data controller" to view captured images. The data controller is responsible for responding to these requests. Police or other law enforcement agencies should produce a standard template request form, setting out the reasons why the disclosure is required. Alternately a signed statement may be accepted.

All requests should only be accepted where they are in writing, specifying the reasons why the disclosure is required.

Under the DPA, members of the public may make a request for the disclosure of images, but only where they have been the subject of a recording. This is known as a 'subject access request'. Such requests must only be accepted where they are in writing and include sufficient proofs of identity (which may include a photograph to confirm they are in fact the person in the recording). Data controllers are also entitled to charge a fee for a subject access request (currently a maximum of £10) as published in the ICO CCTV Code of Practice.

**Signage**

All licensed vehicles with in-vehicle CCTV must display clear and prominent signs advertising the use of in-vehicle CCTV. The driver may also verbally bring to the attention of the passengers that in-vehicle CCTV equipment is in operation within the vehicle, if it is felt appropriate.

The signage must be displayed in such positions so as to minimise obstruction of vision and to make it as visible as possible to passengers, before and after entering the vehicle.
Signs should:-

- Be clearly visible and readable
- Contain details of the organisation/company/individual operating the system, the purpose for using CCTV and who to contact about the scheme
- Be an appropriate size depending on context

To assist individual drivers, owners or companies who are considering installing an in-vehicle CCTV system please use the summary checklist below to ensure all of the approval requirements/standards have been complied with.

- Notification submitted to the Information Commissioner's Office (ICO) Telephone Number: 08456 306060 or 01625545745
- Have the ICO provided you with the documentation to evidence notification of the "data controller" associated with your system?
- Do you have documentary evidence regarding contractual arrangements with any data processor or service provider associated with the CCTV system?
- Does the installed in-vehicle CCTV system meet the installation standards as set out above?
- Do you have satisfactory signage and appropriate contact details displayed?

**Note**
Reference to 'Data Controller', 'Data Processor' and 'Encryption Software' information made in this guideline comply with the current Information Commissioner's Office (ICO0 CCTV Code of Practice 2008).