Report Appendix K

APPENDIX J - In-Vehicle Visual and Audio Recording – CCTV in Hackney Carriage and Private Hire Vehicles

1. Introduction

1.1 This appendix relates to the use of surveillance cameras, also known as Closed Circuit Television (CCTV), in licensed vehicles. The content is designed to facilitate the use of surveillance cameras in licensed vehicles, to protect drivers and passengers, whilst ensuring licence holders respect passenger privacy.

1.2 Proprietors / Operators of vehicles licensed by North Northamptonshire Council will be permitted to voluntarily install CCTV, upon approval under this policy and subject to adherence with this policy throughout the duration of the proprietor's / operator's licence.

1.3 Licence holders are advised that school transport contracts may preclude the installation of CCTV in their vehicle.

1.4 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 surveillance cameras.
- Informing investigations by the Council and police.

1.5 The absence of CCTV in a licensed vehicle does not indicate that the owner of the vehicle has failed to pay attention to passenger or driver safety.

2. Legality

2.1 The ICO and Surveillance Commissioner have given the strongest possible advice that mandatory CCTV is very difficult for licensing authorities to justify.

2.2 The Council considers that CCTV in licensed vehicles as a mandatory requirement would not be proportionate. As such, CCTV is not a licence requirement of North Northamptonshire Council; however, this policy outlines the requirements for those wishing to voluntarily install CCTV.

2.3 This policy has been produced in consideration of The Data Protection Act (2018), General Data Protection Regulations (GDPR) and Article 8 of the European Convention on Human Rights. The policy has regard to The Local

Government Association's 'Developing an approach to mandatory CCTV in licensed vehicles and PHVs'.

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

2.5 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.

3. Compliance, Regulation and Complaints

3.1 The Surveillance Camera Commissioner (SCC) works to encourage compliance with the 'Surveillance camera code of practice'. Licence holders should follow the Surveillance Camera Commissioner's 'Passport to Compliance' to plan, implement and operate a system which complies with the Surveillance Camera Code of Practice. Licence holders are also recommended to obtain third party certification with the Surveillance Camera Commissioner.

3.2 The Information Commissioner's Office (ICO) is the regulatory body responsible for enforcing compliance with privacy and data protection legislation. Licence holders should have regard to the Information Commissioner's Office Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

3.3 If a passenger wants to request CCTV footage relating to them, 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/

3.4 If a passenger has an issue with their 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.

3.5 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/

4. ICO Registration as Data Controller

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

4.2 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.

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

5. Data Processors

5.1 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'.

5.2 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.

6. Audio Recording

6.1 The 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 system that comes equipped with an independent sound recording facility must be turned off or disabled in some other way.

7. Signage and Advising of CCTV

7.1 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 both outside and inside of the windows of every passenger door of the vehicle.

7.2 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. **North Northamptonshire Council is not the Data Controller.**
- The Data Controller's ICO Registration Number.

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

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

8. Storage of Data

8.1 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.

8.2 CCTV footage must be encrypted to prevent unauthorised access. Data should be deleted after thirty-one days, unless it has been legitimately shared, in which case it should be deleted when appropriate on the conclusion of the request.

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

9. Sharing Data

9.1 The licence holder must comply with valid information requests, in consideration of The Data Protection Act (2018) and General Data Protection Regulations (GDPR).

9.2 Data must be shared securely and requests must be fulfilled without charge.

9.3 Data must only be shared where there is a valid lawful reason, for example:

- where a crime report has been made involving the specific vehicle and the Police have formally requested that data.
- 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).
- 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.
- a Subject Access Request (SAR) compliant within the 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 on the ICO website.

9.4 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.

9.5 The uploading of footage to social media does not have a lawful basis and it is expressly prohibited by this policy. This includes, by way of examples, but is not limited to: YouTube, WhatsApp, Instagram, TikTok, Facebook and Twitter. Where licence holders have shared footage, they may be liable to criminal prosecution. Unlawful sharing is a breach of UK Data Protection law and is considered a breach of this policy.

10. Breaches of Policy

10.1 Failure to comply with this appendix to the policy may result in the operator, proprietor and/or vehicle licence being reviewed by the Council.