APPENDIX 4 – STATUTORY STANDARDS – CCTV GUIDANCE

Annex – CCTV Guidance

It is important to note that, in most circumstances, a licensing authority which mandates the installation of CCTV systems in taxis and private hire vehicles will be responsible for the data – the data controller. It is important that data controllers fully consider concerns regarding privacy and licensing authorities should consider how systems are configured, should they mandate CCTV (with or without audio recording). For example, vehicles may not be exclusively used for business, also serving as a car for personal use - it should therefore be possible to manually switch the system off (both audio and visual recording) when not being used for hire. Authorities should consider the Information Commissioner's view on this matter that, in most cases, a requirement for continuous operation is unlikely to be fair and lawful processing of personal data.

The Home Office 'Surveillance Camera Code of Practice' https://www.gov.uk/government/publications/surveillance-camera-code-of-practice advises that government is fully supportive of the use of overt surveillance cameras in a public place whenever that use is:

- in pursuit of a legitimate aim;
- necessary to meet a pressing need;
- proportionate;
- effective, and;
- compliant with any relevant legal obligations

The Code also sets out 12 guiding principles which, as a 'relevant authority' under section 33(5) of the Protection of Freedoms Act 2012, http://www.legislation.gov.uk/ukpga/2012/9/section/33/enacted licensing authorities must have regard to. It must be noted that, where a licence is granted subject to CCTV system conditions, the licensing authority assumes the role and responsibility of 'System Operator'. The role requires consideration of all guiding principles in this code. The failure to comply with these principles may be detrimental to the use of CCTV evidence in court as this may be raised within disclosure to the Crown Prosecution Service and may be taken into account.

The Surveillance Camera Commissioner (SCC) has provided guidance on the Surveillance Camera Code of Practice in its 'Passport to Compliance' https://departmentfortransportuk.sharepoint.com/sites/BusTaxi/Taxis/Control%20of%20Taxis%20and%20PHV/STATUTORY%20GUIDANCE%20(2019)/FINAL%20VERSION%20DOCUMENTS%20(2019)/government/public which provides guidance on the necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the code. The Information Commissioner's Office (ICO) has also published a code of practice https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf which, in this context, focuses on the data governance requirement associated with the use of CCTV such as data retention and disposal, which it is important to follow in order to comply with the data protection principles. The SCC provides a self-assessment tool to assist operators to ensure compliance with the principles set of in the Surveillance Camera Code of Practice. The SCC also operate a certification scheme; authorities that obtain this accreditation are able to clearly demonstrate that their systems conform to the SCC's best practice and are fully compliant with the Code

https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool and increase public confidence that any risks to their privacy have been fully considered and mitigated.

The Data Protection Act 2018 regulates the use of personal data. Part 2 of the Data Protection Act applies to the general processing of personal data, and references and supplements the General Data Protection Regulation. Licensing authorities, as data controllers, must comply with all relevant aspects of data protection law. Particular attention should be paid to the rights of individuals which include the right to be informed, of access 39 and to erasure. The ICO has provided detailed guidance on how data controllers can ensure compliance with these.

It is a further requirement of data protection law that before implementing a proposal that is likely to result in a high risk to the rights and freedoms of people, an impact assessment on the protection of personal data shall be carried out. The ICO recommends in guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ that if there is any doubt as to whether a Data Protection Impact Assessment (DPIA) is required one should be conducted to ensure compliance and encourage best practice. A DPIA will also help to assess properly the anticipated benefits of installing CCTV (to passengers and drivers) and the associated privacy risks; these risks might be mitigated by having appropriate privacy information and signage, secure storage and access controls, retention policies, training for staff how to use the system, etc.

It is essential to ensure that all recordings made are secure and can only be accessed by those with legitimate grounds to do so. This would normally be the police if investigating an alleged crime or the licensing authority if investigating a complaint or data access request.

Encryption of the recording to which the licensing authority, acting as the data controller, holds the key, mitigates this issue and protects against theft of the vehicle or device. It is one of the guiding principles of data protection legislation, that personal data (including in this context, CCTV recordings and other potentially sensitive passenger information) is 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.

All passengers must be made fully aware if CCTV is operating in a vehicle. Given that audio recording is considered to be more privacy intrusive, it is even more important that individuals are fully aware and limited only to occasions when passengers (or drivers) consider it necessary. The recording of audio should be used to provide an objective record of events such as disputes or inappropriate behaviour and must not be continuously active by default and should recognise the need for privacy of passengers' private conversations between themselves. Activation of the audio recording capability of a system might be instigated when either the passenger or driver operates a switch or button. As well as clear signage in vehicles, information on booking systems should be introduced. This might be text on a website, scripts or automated messages on telephone systems; the Information Commissioner's Office (ICO) has issued guidance on privacy information and the right to be informed on its website