CCTV in Hire Cars

Report by Director, Resources

1 Purpose of Report

To seek authority to proceed with the introduction of permitting the installation of CCTV in Taxis and Private Hire Cars.

2 Background

On 1 April 2014, the Committee approved in principle the introduction of a policy that will permit the installation of CCTV in Taxis and Private Hire Cars.

Discussions have taken place with the Information Commissioner who has drafted a revision to the existing CCTV Code of Practice and issued it for public consultation. From the responses they have received, it appears that they are unlikely to make substantive changes so the consultation draft can be used to inform policy direction and practice.

In section 8 of the consultation draft, the ICO recommends that audio recording should only be undertaken in particular circumstances and this could also apply to video recording. The most relevant to CCTV in taxis would be where the recording system is activated due to a sudden change in noise level, suggesting that an argument may have started, or in response to the driver triggering the recording by activating a 'panic button'. The ICO also recommends that a privacy impact assessment is undertaken as part of the development of this policy to identify the best way to protect people's privacy.

The data controller for the recorded personal data will be the person or organisation who actually controls that data. If the Council decides which system is to be used, provides instructions on when and how to use it, decides who can access the footage and in what circumstances, and decides when to destroy footage and is responsible for doing so, then it would be the data controller. However, if taxi companies or drivers as sole traders can choose their own system and are responsible for the other aspects, then they will be the data controller for the purposes of the Act. It is not possible to confer data controller status on another organisation to abdicate the Council's responsibilities. If the Council does determine which system to use and what happens to the data so that it is the data controller, it will then be liable for any enforcement action the Information Commissioner decides to take in the event of a serious breach.

In respect of Glasgow City Council's policy in this regard, the ICO were asked to provide comments on the policy when it was in draft but had very little to say as it seemed to cover all the bases quite well.

There is information contained in **Appendix 1** relating to Privacy Impact Assessments (PIAs).

An overview of the PIA Process is shown in **Appendix 2**

A draft outline policy based on the Glasgow one is shown at **Appendix 3.**

3 Report Implications

3.1 Resource
There are no resource implications arising directly from this report.

3.2 Risk
There are no risk implications arising directly from this report.

3.3 Single Midlothian Plan and Business Transformation
Themes addressed in this report:

☒ Community safety
☐ Adult health, care and housing
☐ Getting it right for every Midlothian child
☐ Improving opportunities in Midlothian
☐ Sustainable growth
☐ Business transformation and Best Value
☐ None of the above

3.4 Key Priorities within the Single Midlothian Plan
There are implications arising directly from this report.

3.5 Impact on Performance and Outcomes
There are no implications arising directly from this report.

3.5 Adopting a Preventative Approach
There are no implications arising directly from this report.

3.6 Involving Communities and Other Stakeholders
The Hire Car Associations were consulted.

3.7 Ensuring Equalities
There are no implications arising directly from this report.

3.8 Supporting Sustainable Development
There are no implications arising directly from this report.

3.9 IT Issues
There are no implications arising directly from this report.

4 Summary

The introduction of CCTV in Hire Cars is supported by the Trade.

The Policy is being introduced for reasons of public safety.

A Privacy Impact Assessment may require to be carried out. However, since the individual licence- holders will be the Data Controllers, the onus may be on them to carry out that responsibility.

Authority is requested to proceed with the implementation of a Scheme that will provide, *inter alia*, that :-

(a) footage or images must be securely stored at all time and never downloaded to portable devices such as memory sticks or CDs;

(b) images or audio recording captured by CCTV must be retained for no longer than 31 days;

(c) a sign indicating that a CCTV / Audio recorder is in use and the contact number of the licence holder, must be clearly displayed;

(d) Passengers must be advised by the driver that a CCTV / Audio recorder is in use;

(e) Police, Licensing Officers and Insurance Investigators must request permission, in writing, to view footage or images / listen to audio recording; and

(e) only those who are the subject of a recording are permitted to view footage or images or listen to audio recordings.

5 Recommendation

It is recommended that the Committee approve the Policy shown in **Appendix 3**, subject to consultation with the Trade**.**

Date 23 September 2014

Report Contact:
Name Bob Atack Tel No 0131 271 3161
atackb@midlothian.gov.uk

APPENDIX 1

Privacy impact assessments (PIAs)

Privacy impact assessments (PIAs) are a tool that can be used to identify and reduce the privacy risks of the project. A PIA can reduce the risks of harm to individuals through the misuse of their personal information; and also help in the design of more efficient and effective processes for handling personal data. The core principles of the PIA process can be integrated with the development of the policy and risk management aspects. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout the Council.

The ICO have published a Conducting privacy impact assessments code of practice which explains what PIAs are and how they can be used. The code contains annexes which can be used as the basis for the PIA. These include questions to guide the process and templates for recording the assessment. It is not necessary to use these if the Council's own processes are preferred, but the annexes are included here in an editable format.

As part of the ICO's work in this area, they commissioned a report into the use of PIAs and the potential for further integration with project and risk management. The report was drafted by Trilateral Research and Consulting. the report and an executive summary can be accessed here.

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information

- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

The code is concerned primarily with informational privacy, but an organisation can use PIAs to assess what they think are the most relevant aspects of privacy.

Privacy risk is the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:-

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job.

At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk. An organisation will need to develop an understanding of how it will approach the broad topics of privacy and privacy risks. There is not a single set of features which will be relevant to all organisations and all types of project - a central government department planning a national crime prevention strategy will have a different set of issues to consider to an app developer programming a game which collects some information about users.

Identifying the need for a PIA

- Answer screening questions to identify a proposal's potential impact on privacy.
- Begin to think about how project management activity can address privacy issues.
- Start discussing privacy issues with stakeholders.
- Conducted early during the project planning stage
- The overall aims of the project are described
- The project development process is adapted to address privacy concerns

Describing information flows

- Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)
- People who will be using the information are consulted on the practical implications.
- Potential future uses of information are identified, even if they are not immediately necessary.

Identifying privacy and related risks

□□Record the risks to individuals, including possible intrusions on privacy where appropriate.
□□Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust.
□□Conduct a compliance check against the Data Protection Act and other relevant legislation.
□□Maintain a record of the identified risks.
□□The process helps an organisation to understand the likelihood and severity of privacy risks.
□□An organisation is open with itself about risks and potential changes to a project.

Identifying and evaluating privacy solutions

□□Devise ways to reduce or eliminate privacy risks.
□□Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.
□□Refer back to the privacy risk register until satisfied with the overall privacy impact.
□□The process takes into account the aims of the project and the impact on privacy.
□□The process also records privacy risks which have been accepted as necessary for the project to continue.

Signing off and recording the PIA outcomes

□□Obtain appropriate signoff within the organisation.
□□Produce a PIA report, drawing on material produced earlier during the PIA.
□□Consider publishing the report or other relevant information about the process.
□□The PIA is approved at a level appropriate to the project.
□□A PIA report or summary is made available to the appropriate stakeholders.

Integrating the PIA outcomes back into the project plan

Ensure that the steps recommended by the PIA are implemented.
□□Continue to use the PIA throughout the project lifecycle when appropriate.
□□The implementation of privacy solutions is carried out and recorded.
□□The PIA is referred to if the project is reviewed or expanded in the future.

Overview of the PIA process	
1. Identifying the need for a PIA. The need for a PIA can be identified as part of an organisation's usual project management process or by using the screening questions in annex two of this Code.	2. Describing the information flows. Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information
3. Identifying the privacy and related risks. Some will be risks to individuals - for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy. Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach. Legal compliance risks include the DPA, PECR, and the Human Rights Act.	4. Identifying and evaluating privacy solutions. Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy. Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.
5. Signing off and recording the PIA outcomes. Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval. A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks. Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.	6.Integrating the PIA outcomes back into the project plan. The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process. A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored. Record what you can learn from the PIA for future projects.

Appendix 3

POTENTIAL POLICY FOR CCTV IN HIRE CARS

The aim of this policy is to allow for the safe installation and use of CCTV systems in taxis and private hire cars licensed by Midlothian Council's Licensing Authority. In allowing the installation and use of CCTV, the Licensing Authority recognises that such systems can be used to prevent and detect crime, reduce the fear of crime and enhance the safety of taxi and private hire car drivers, as well as their passengers. However, this policy also seeks to ensure that the installation and operation of CCTV systems do not compromise the safety of either drivers or passengers or unreasonably interfere with the privacy of members of the public. For the purposes of this policy, a CCTV system will include any electronic recording device attached to the inside of a taxi or private hire car having the technical capability to capture and retain visual images from inside or external to the vehicle.

This policy does not place a mandatory requirement on the licensed operators of taxis and private hire cars to install CCTV systems in their vehicles. Any CCTV system to be fitted in a taxi or private hire car must, as a minimum, meet the requirements of this policy. Only CCTV systems meeting these requirements can be installed into licensed taxis and private hire cars. Where an operator wishes to install and use a CCTV system, it will be a condition of the taxi or private hire car licence that the requirements of this policy are complied with. Failure to comply with the requirements of this policy could lead to a complaint being made to the Licensing and Regulatory Committee in order to consider the possible suspension of the licence.

THE DATA CONTROLLER

The Information Commissioner defines a "data controller" as the body which has legal responsibility under the Data Protection Act 1998 for all matters concerning the use of personal data. For the purpose of the installation and operation of a CCTV system in taxis and private hire cars, the "data controller" will be the holder of the taxi or private hire car licence and not the driver. The licence holder, as data controller, will therefore be responsible for ensuring compliance with the requirements of this policy and with all relevant data protection legislation, including the Data Protection Act 1998. The data controller is legally responsible for the use of all images including breaches of legislation.

THIRD PARTY 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 the data processor. The contract must contain provisions covering security arrangements, retention/deletion instructions, access requests and termination arrangements. A copy of the contract must be provided to an authorised officer of the Licensing Authority, or to the Police, on reasonable request.

GENERAL REQUIREMENTS – INSTALLATION AND OPERATION

CCTV systems must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified except in very exceptional circumstances. Wherever possible, the CCTV system should not have any sound recording facility. However, if the system comes equipped with a sound recording facility then this functionality should be disabled and only capable of being utilised in the following limited circumstances:-

Audio recording will only be justified where the recording is triggered due to a specific threat to driver or passenger safety, e.g. a 'panic button' is utilised and must be subject to the following safeguards:-

a) Where this audio recording facility is utilised a reset function must be installed which automatically disables audio recording and returns the system to normal default operation after a specified time period has elapsed.

b) The time period that audio recording may be active should be the minimum possible and should be declared at the time of submission for approval of the equipment.

In the limited circumstance where audio recording is justified, signs must make it very clear that audio recording is being or may be carried out.

CCTV systems installed in taxis and private hire cars will be inspected as part of the annual and intermediate inspections carried out by the Taxi and Private Hire Car Inspection Centre.

The installation and operation of a CCTV system must comply with the requirements of the Information Commissioner's CCTV Code of Practice, which is available at the following address:-

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 any and all requirements as regards safety, technical acceptability and operational/data 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 to the 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. In particular, the camera(s) must be fitted safely and securely in such a way that it does not adversely encroach into the passenger area and must not impact on the safety of the driver, passenger or other road users. All equipment must be installed as prescribed by the equipment and/or vehicle manufacturer installation instructions by a qualified auto-electrician.

The 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. For example, temporary fixing methods such as suction cups will not be permitted, or lighting, such as infra-red, which emits at such a level that may cause distraction or nuisance to the driver and/or passengers.

All equipment must be protected from the elements, secure from tampering and located such as to have the minimum intrusion into any passenger or driver 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/air curtains 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.

The location of the camera(s) installed within the vehicle must be for the purpose of providing a safer environment for the benefit of the taxi or private hire car driver and passengers, and not for any other purpose.

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.

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 an 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 therefore must meet with requirements specified in that Directive.

CCTV equipment should be e-marked or CE-marked. If CE marked confirmation by the equipment manufacturer as being non-immunity related and suitable for use in motor vehicles is required.

Activation of the equipment may be via a number and combination of options, such as - door switches, time delay, drivers' panic button or in the case of incident/event recorder, predetermined G-Force parameters set on one or more axis (i.e. braking, acceleration, lateral forces) and configured to record for a short period of time before the event, during the event and a short period following the event.

SECURITY OF IMAGES

All Images captured by the CCTV system must remain secure at all times.

The captured images must be protected using 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 that the data controller ensures that 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 CCTV equipment selected for installation must have the capability 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.

The CCTV system must include an automatic overwriting function, so that images are only retained within the installed 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.

Where applicable, these provisions shall also apply to audio recordings.

USE OF INFORMATION RECORDED USING CCTV

Any images and any audio recording should only be used for the purposes described in this policy.

Requests may be made to the data controller by Authorised Officers of the Licensing Authority, the Police or other statutory law enforcement agencies, insurance companies / brokers / loss adjusters or exceptionally other appropriate bodies, to view captured images, or obtain audio recordings if applicable. The licence holder, as data controller, is responsible for responding to these requests. Police, Authorised Officers of the Licensing Authority or other law enforcement agencies should produce a standard template request form, setting out the reasons why the disclosure is required. Alternatively a signed statement may be accepted.

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

Under the Data Protection Act 1998, members of the public may also 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 Information Commissioner's CCTV Code of Practice.

SIGNAGE

All taxis and private hire cars with CCTV must display signage within the vehicle to indicate that CCTV is in operation. The driver must also verbally bring to the attention of the passengers that CCTV equipment is in operation within the vehicle.

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.

In the limited circumstance where audio recording is justified, signs must make it very clear that audio recording is being or may be carried out and this must also be verbally brought to the attention of the passengers.

CONTACT DETAILS

The name and the contact telephone number of the licence holder, as data controller must be included on the sign.

SIGNAGE FOR EXTERNAL FACING CCTV SYSTEMS

Where a CCTV system is installed within the vehicle in order to record incidents *outside of* the vehicle, it will not be practical to display a sign. Instead, when the CCTV is activated in response to an incident, the driver of the vehicle must inform the person(s) recorded that their personal data was captured - as soon as practicable after the incident.

They should also be informed of the purpose for which the device has been installed, being driver and passenger safety.

Declaration Box

Instructions: This box must be completed by the author of the report. The box will be copied and saved by the Council Secretariat who will delete it from the report prior to photocopying the agenda.

Title of Report:

Meeting Presented to:

Author of Report:

I confirm that I have undertaken the following actions before submitting this report to the Council Secretariat (Check boxes to confirm):-

☐ *All resource implications have been addressed. Any financial and HR implications have been approved by the Head of Finance and Integrated Service Support.*
☐ *All risk implications have been addressed.*
☐ *All other report implications have been addressed.*
☐ *My Director has endorsed the report for submission to the Council Secretariat.*

For Cabinet reports, please advise the Council Secretariat if the report has an education interest. This will allow the report to be located on the Cabinet agenda among the items in which the Religious Representatives are entitled to participate.

Likewise, please advise the Council Secretariat if any report for Midlothian Council has an education interest. The Religious Representatives are currently entitled to attend meetings of the Council in a non-voting observer capacity, but with the right to speak (but not vote) on any education matter under consideration, subject always to observing the authority of the Chair.