Local Government Association

Developing an approach to mandatory CCTV in taxis and PHVs

Guidance

Foreword

Councils work hard to ensure that only those fit to drive taxis and private hire vehicles (PHVs) are licensed to do so, and the vast majority of drivers across the country work hard to provide a good service to their passengers, many of whom rely on this vital service.

However, we cannot avoid the fact that over recent years there have been a number of high profile cases of licensed drivers abusing their passengers' trust, including serious cases of child sexual exploitation (CSE).

It is vital that licensing teams understand how they can contribute to the safeguarding agenda. We have various tools at our disposal to enhance safeguarding in our licensing work, including introducing a requirement for CCTV systems in licensed vehicles.

A number of councils have taken the decision to mandate CCTV systems, whether cameras or cameras and audio recording, as a way to further safeguard passengers and drivers. First and foremost, the presence of CCTV acts as a deterrent to criminal or other poor behaviour, but it also provides vital evidence in situations where an incident has been reported, which otherwise may have been one person's word against another.

It is incumbent on all of us to review our policies and procedures to make certain we are taking all possible steps and using the tools available to us to protect the vulnerable. We have developed this guidance to bring together some of the questions that authorities may want to consider if they are thinking about introducing a mandatory CCTV policy for licenced vehicles in their area.

The guidance reflects on approaches taken by authorities which already mandate CCTV and on the importance of striking a balance between passenger safety and privacy, reflecting the position of the Information Commissioner and Surveillance Camera Commissioner as the regulators. It is intended to be used as a starting point for exploring some of the key issues and how these might apply at a local level.

We hope you find it useful.

Councillor Simon Blackburn
Chair, LGA Safer and Stronger Communities Board

Contents

Introduction 4

Overview – benefits and challenges of CCTV in taxis/PHVs 6

Developing an approach to CCTV 10

Consultation and engagement 12

Data protection, privacy and information governance 13

- The regulatory framework 13
- Information governance 16

Implementation and enforcement 22

Appendices 25

- Flow chart 25
- Glossary 26
- Links to useful resources and guidance 27

Introduction

Taxis and private hire vehicles (PHVs) are a vital part of local transport networks. Alongside their importance to the local night-time and visitor economies in particular, they are a key way of supporting more vulnerable local residents; for example by transporting children to and from school or providing a door-to-door service for elderly and disabled users, many of whom would otherwise struggle to access local amenities. The number of journeys made using taxis/PHVs continue to rise and in 2018 the number of licenced vehicles reached a record high of 285,400.

The key role of licensing authorities is to ensure a safe and effective local taxi and PHV service and, following recent cases where taxis and PHVs were used to facilitate appalling instances of child sexual exploitation (CSE) this area of councils' work has been under intense scrutiny. Both Professor Alexis Jay and Dame Louise Casey CB's reports into CSE in Rotherham highlighted the vital role that effective regulatory and enforcement functions play in preventing and disrupting CSE. In response, councils have been reviewing existing taxi and PHV licensing policies to ensure the right measures are in place to protect members of the public when using taxis/PHVs.

As part of broader work to strengthen safeguarding measures within the taxi/PHV service, some licensing authorities have begun to look at the use of in-vehicle cameras and audio recording (CCTV systems) and a small number of authorities already mandate the use of CCTV systems in licenced vehicles.[1]

Many more councils allow the use of CCTV systems in taxis/PHVs or have a voluntary scheme in place – latest figures[2] from the Department for Transport (DfT) show around 95 per cent of councils allow the use of CCTV in taxis/PHVs.

Whilst there has been relatively little guidance published which relates specifically to the use of CCTV in taxis/PHVs, there is a range of more general advice which it is important for authorities to be aware of. The Protection of Freedoms Act 2012 (PoFA) implemented the Home Secretary's Surveillance Camera Code of Practice (SC Code)[3] which provides guidance on the appropriate and effective use of surveillance camera systems by 'relevant authorities' and is particularly significant. As relevant authorities (under s.33 of the Protection of Freedoms Act 2012) licensing authorities have a statutory duty to demonstrate regard to the SC Code where cameras are deployed in public places[4], which includes taxis/PHVs.

The SC Code is designed to provide a framework for those operating and using surveillance camera systems to ensure use of surveillance is proportionate and transparent, and the systems used are capable of providing good quality images (or other information) which are fit for purpose.

1 Licensing authorities who have mandated cameras in vehicles are: Brighton and Hove, East Riding, Exeter, Gravesham, Portsmouth, Warrington and Worthing. Those mandating both cameras and audio are: Cambridge, Herefordshire, Rossendale, Rotherham, and Southampton.

2 www.gov.uk/government/statistics/taxi-and-private-hire-vehicle-statistics-england-2018

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

4 'Public place'" has the meaning given by S.16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.

The code sets out 12 guiding principles and where a licensing authority is considering mandating CCTV systems in taxis/PHVs they must have particular regard to guiding principle one, which is: 'Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need'. The code is clear that a mandatory policy around CCTV systems in taxis will require strong justification and should be kept under regular review.

Reference to the use of CCTV systems in taxis/PHVs is made in existing best practice guidance published by the Department for Transport (DfT) in 2010, which suggests that local authorities encourage its use. It is likely that the DfTs new statutory/best practice guidance, due for consultation in early 2019 will say more about the use of CCTV in taxis and PHVs in relation to the role it can play in safeguarding both passengers and drivers.

Terminology

Some local authorities use the term taxi camera, instead of CCTV as they feel this may be misleading to the public, invoking the idea of surveillance and suggesting that footage is being monitored live. However, for clarity we use the term CCTV throughout this document.

Purpose of LGA guidance

Amongst those councils that already mandate CCTV systems, there is a range of different requirements around how and when the systems are used, and the types of systems that can be fitted. It is important that individual licensing authorities make their own decisions about what the best approach to CCTV is, based on the local context. The intention of the Local Government Association's (LGA) guidance is to outline some of the key issues to consider for authorities who are exploring mandating the use of CCTV systems in taxis/PHVs.

The guidance aims to help local authorities to comply with their legal responsibilities when considering mandating CCTV and is based on guidance from key organisations such as the Information Commissioner's Office (ICO), the Surveillance Camera Commissioner (SCC) and the experience of councils who already require CCTV in taxis/PHVs. The document also touches on some of the ongoing debates about the proportionality of requiring CCTV. The guidance reflects changes to legislation brought in by the General Data Protection Regulation (GDPR), implemented in the UK via the Data Protection Act (DPA) 2018.

The document is more heavily weighted towards the practical issues that councils will need to consider in implementing a mandatory approach to CCTV, rather than the safeguarding justification for doing so. This is because councils will need to make their own assessment of whether CCTV is the right solution based on the local context.

This guidance makes reference to a number of licensing authorities which have already mandated the use of CCTV. We thank all the councils involved in the development of this document for their help.

Alongside reading this guidance, authorities may also wish to consult experts within your councils about the deployment of CCTV in taxis/PHVs; this could be the person who manages your town centre CCTV scheme and/or your data protection officer.

Overview – benefits and challenges of CCTV in taxis/PHVs

There is an inherent, structural vulnerability relating to taxis and PHVs: getting into a taxi/PHV, an individual puts themselves under the control of a stranger in a confined space with no physical control over where they are taken. The primary role of the licensing regime is to manage this risk, in particular by satisfying themselves that only those who are fit and proper to do so hold a licence.

CCTV systems can act as an additional safeguard, providing protection, confidence and reassurance to the public when they are travelling in a taxi or PHV as well as to drivers, who can also be victims of violence and abuse. Mandating CCTV has been seen by some authorities as a proactive preventative measure that can be taken to protect passengers and drivers. It can act as a deterrent to committing an offence as people are more likely to police their own behaviour. Where an offence has taken place the images/audio recording that CCTV systems capture can provide important evidence in a criminal investigation.

Some licensing authorities have introduced voluntary, rather than mandatory, CCTV schemes. However there is evidence that there has been limited take up of these, even where authorities have offered to pay for a percentage of installing the system. Mandating CCTV will by definition ensure greater take up, and can also lead to greater consistency, with authorities able to set out and oversee clear specifications, guidelines and procedures on a range of issues including the type of systems used and information governance.

Sheffield pilot scheme

Following a string of attacks against drivers in the city, in December 2006 Sheffield piloted a CCTV scheme. The pilot involved 33 vehicles (eight taxis and 25 PHVs) and ran for six weeks, three weeks without cameras and three weeks with a camera fitted, with drivers reporting back at the end of the six week trial.

A subsequent report based on drivers' feedback suggested that there had been a large reduction in incidents from an average of one in seven fares to less than one in 100 fares, with a very significant reduction in incidents of threats and violence. In addition to the benefit to drivers there was some positive anecdotal feedback from passengers, particularly lone females, who said that they felt safer when there was a camera installed.

Report of the Sheffield taxi safety camera pilot study (February 2007) www.calderdale.gov.uk/nweb/COUNCIL.minutes_pkg.view_doc?p_Type=AR&p_ID=3412

Key considerations

It is useful be aware of some of the key considerations as well as challenges that councils may face with plans to introduce mandatory CCTV systems both from members of the public, regulators and the trade.

Views of the trade

Many areas across the country will have active taxi/PHV trade groups or associations who may oppose plans to mandate the use of CCTV systems. Reasons could include the financial burden of installing CCTV systems that meet the agreed specification or invasion of drivers' privacy. It is therefore important to work with the trade as early as possible when considering a policy on CCTV systems, and ensure that key messages around why this approach is being considered, and the potential benefits to drivers, are clearly communicated. Issues raised by the trade can then be considered and where possible addressed as plans develop.

Sections of the taxi/PHV trade have already challenged some licensing authorities around mandatory CCTV. In some cases legal challenges have been brought. However, at the time of writing, magistrates have so far rejected challenges where councils were able to demonstrate that they had taken issues raised by the trade into consideration when developing policies.

The intrusive capabilities of CCTV means that there will need to be careful consideration of the impact it will have on privacy and how it can be used in a way that is sensitive and transparent so as to maintain both drivers and the public's confidence in its use. Proposals will need to clearly set out how privacy issues have been considered and how any issues raised have been mitigated. Consideration of these issues will need to be demonstrated through a data protection impact assessment (DPIA), which is required to be carried out before the roll-out of any intrusive surveillance system, including CCTV. The Surveillance Camera Commissioner has worked with the Information Commissioner's Office to develop a surveillance camera specific impact assessment template (updated in October 2018) available on the Surveillance Camera Commissioner's website.[5] Both privacy issues and legal requirements around data protection are discussed in full later in this guidance.

5 www.gov.uk/government/publications/privacy-impact-assessments-for-surveillance-cameras

Whilst the focus is often on how CCTV systems positively impact on passenger safety, there is also a strong argument for the benefits it has for drivers' safety. As well as acting as a deterrent, CCTV systems will also help to provide evidence in case of an incident being reported. Authorities will be familiar with cases where an incident has been reported by a passenger relating to a drivers conduct or vice versa which are extremely difficult to prove. Footage from CCTV systems can provide vital evidence, and even prevent drivers from losing their licence if an accusation is proven to be false. However, compliance with the PoFA and the SC Code is vital if CCTV evidence is to be used in court.

In some places the trade have actively called for the council to introduce CCTV in taxis/PHVs to protect drivers' safety. Whilst based on only a small sample, analysis of a pilot scheme in Sheffield (see case study, page 6) suggested that, where taxis/PHVs were fitted with CCTV systems, there was a significant reduction in incidents. More recently in 2012, Brighton and Hove Council surveyed drivers asking whether they agreed with the current policy of all vehicles having CCTV, six months after the policy was introduced. Seventy-two per cent of hackney carriage drivers and fifty four per cent of private hire respondents were supportive of the policy.[6]

Early engagement with the trade can be useful in understanding their experiences and what particular issues they face in the local area, information gathered can form part of an evidence base for a policy and DPIA. This will also ensure compliance with guiding principle three[7] of the SC Code which requires meaningful consultation with groups impacted upon by CCTV. Collating statistics and any incident data relating to taxis/PHVs from your local police force will also help to build a picture of the local context to inform an impact assessment.

6 See page 119 https://present.brighton-hove.gov.uk/Published/C00000116/M00004177/AI00030770/Enc1forHackneyCarriageUnmetDemandSurveyv2.pdf

7 There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

Other benefits to drivers of installing CCTV include the potential to realise savings on insurance premiums, which may help to offset the upfront cost of purchasing and installing the systems. For example, some insurance providers have offered drivers who have forward facing cameras fitted in addition to the interior ones, a reduction to their insurance premiums of around 10 –to 15 per cent (a saving of around £200-£250 per year). Rotherham estimated that the average saving on insurance would pay for the cost of the CCTV system within two years. The initial cost of CCTV systems can also be offset against tax (for those drivers who reach the income tax threshold).

In practical terms considering the cost of CCTV systems and how this can be managed is something that can be done as part of an implementation schedule discussed on page 24. Giving drivers enough of a lead-in time before CCTV systems have to be fitted will enable them to save up or stagger the cost.

Privacy and proportionality

The use of CCTV is intrusive and its use is subject to data protection and human rights laws. Members of the public, drivers, the Surveillance Camera Commissioner (SCC) and the Information Commissioners Office (ICO) may all raise concerns about the impact of mandatory CCTV systems on privacy, and this has been a key issue for licensing authorities that have already mandated CCTV in taxis/PHVs.

The Surveillance Camera Commissioner's blog on CCTV in taxis[8] provides a useful summary of the broad legislative framework that local authorities need to consider, including the Data Protection Act 2018 (DPA) and the PoFA 2012. The Commissioner's speech to the National Association of Taxi Drivers in 2015 also provides helpful context.[9]

Councils will need to think through the privacy implications of mandating CCTV and satisfy themselves that where they choose to mandate CCTV, they have adequate justification for choosing this approach and that they meet the requirements of legislation and associated codes of practice on privacy, proportionality and data protection. However, while there are steps that can be taken to try to ensure compliance with the overarching framework and codes, licensing authorities will ultimately be making an assessment about what they consider to be proportionate in balancing the right to privacy with duties to safeguard the public. There are various tools provided by the SCC which will help when considering the implementation of CCTV in taxis including the Buyers' Toolkit[10] which is an easy-to-follow guide for non-experts who are considering the use of a CCTV system, and the Passport to Compliance[11] which is a set of documents that will guide authorities through the relevant principles within the SC Code and will help to ensure a system complies with the code.

Different authorities may take different views on CCTV and what is considered to be a proportionate approach may differ from one area to another, depending on the local context: each policy and DPIA should be explicitly linked to local circumstances.

Some authorities have implemented policies that require mandatory CCTV only when a vehicle is in use as a taxi or PHV, ie there is a 'switch off' facility for when a vehicle is being used for private purposes. Others have sought a 24/7 approach in which CCTV automatically operates when an engine is running, regardless of whether there is a passenger in the vehicle. It is worth noting that the Information Commissioner has addressed this specific point in a recent blog post[12] suggesting that a requirement for continuous recording when a vehicle is being used in a private capacity is likely to

8 https://videosurveillance.blog.gov.uk/2018/08/28/cctv-in-taxis-are-you-talking-to-me

9 www.gov.uk/government/speeches/surveillance-camera-commissioners-speech-to-the-national-taxi-association-agm

10 www.gov.uk/government/publications/surveillance-camera-commissioners-buyers-toolkit

11 www.gov.uk/government/publications/passport-to-compliance

12 https://ico.org.uk/about-the-ico/news-and-events/blog-continuous-cctv-in-taxis-where-do-councils-stand

be unlawful and unfair. Where the ICO has been made aware of councils implementing this approach, they have advised that the requirement for continuous recording is likely to be disproportionate to the problem it is trying to address.

Authorities may also take different approaches to the use of audio recording, which is generally considered by the ICO to be more invasive of privacy than cameras and will therefore require much greater justification.

These are issues about which there are different and, to some extent, philosophical views about what constitutes the appropriate balance between privacy and safeguarding. The ICO has looked closely at, and previously challenged, some licensing authorities on the CCTV policies they have implemented where it believes these go too far in terms of invasion of privacy or have not been adequately justified. This is discussed later on.

Therefore, although determining what is proportionate will need to be assessed by individual councils, looking at areas that have already mandated CCTV is helpful in indicating the balance that has been taken elsewhere. Councils will need to ensure when considering what is an appropriate and proportionate approach to CCTV that this is based on evidence of issues identified in the local area.

The next chapter provides more detail about data protection, privacy and information governance but the key point is that during the process of developing a proposal for mandatory CCTV systems, authorities will need to demonstrate that thought has been given to what the impacts on privacy might be and, where necessary, how these can be mitigated.

Likewise once a decision has been made to introduce mandatory CCTV, careful consideration needs to be given to the processes and procedures that are put in place to safeguard the data captured to ensure compliance with data protection legislation as well as the Protection of Freedoms Act 2012 and other relevant legislation.

The role of councillors

The close involvement of councillors and ensuring there is political buy-in throughout the policy development process is vital and councillors will need to be equipped with the evidence they need to determine whether or not mandatory CCTV is appropriate. Councillors' key role in providing political accountability for decisions is particularly important where proposals may attract some opposition. Several areas have had significant pushback from the taxi and PHV trade which includes members coming under pressure from these groups. In areas that have mandated CCTV, political support has been extremely important in delivering new policies.

Whilst the trade are a vital part of the local economy, it is important to remember that passengers should be at the centre of a licensing authority's taxi licensing policies and processes, something which was highlighted in Dame Louise Casey's review into Rotherham, which noted; 'The safety of the public should be the uppermost concern of any licensing and enforcement regime: when determining policy, setting standards and deciding how they will be enforced.'[13]

Ultimately it will be councillors who should make a decision around mandating CCTV in taxis/PHVs so officers will need to ensure they have the necessary information to make an informed decision. The SCC has produced a guide to the SC Code which is available on his website.[14]

13 See page 103 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401125/46966_Report_of_Inspection_of_Rotherham_WEB.pdf

14 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/498895/SCC_Councillors_Guide_-_February_2016.pdf

Developing an approach to CCTV

The data protection impact assessment (DPIA)

The General Data Protection Regulation (GDPR) states that a data protection impact assessment (DPIA) must be carried out prior to the roll-out of any intrusive surveillance system. CCTV in taxis and licensed vehicles is likely to be one such system and authorities will need to be able to demonstrate that they have conducted a DPIA to the ICO.[15]

The critical starting point is for licensing authorities to be very clear about the problem that needs to be addressed and be able to justify why they consider mandating CCTV in taxis/ PHVs to be an effective solution. Authorities may want to show why CCTV, rather than a potentially less intrusive solution, is required. This is a key component of principle one of the SC Code and the SCC's Buyer's Toolkit[16] can help determine the justification for CCTV in taxis or whether there may be another solution to issues that have been identified.

Where councils have identified that CCTV may be a suitable option, they will need to consider what the appropriate approach to this is. This will necessarily start with developing a rationale for mandating CCTV, relevant to the local context and lead on to considerations about whether there is a need for both camera and audio recording, and when these may be required to operate.

Councils may feel that the inherent vulnerability relating to taxis/PHVs where sometimes vulnerable people are unaccompanied in a car with a stranger means that mandatory CCTV can be justified as a proactive and preventative measure. However, the ICO and SCC are unlikely to consider that the simple basis of high profile CSE cases in Rotherham and elsewhere as being a proportionate justification for implementing CCTV in other parts of the country.

The assessment of proportionality and the justification for this needs to be relevant to the local circumstances in which the policy will apply, so a local evidence base will need to be developed to support any proposal. This could include data from the licensing team around any specific cases where the presence of CCTV could have been beneficial, or any intelligence or incident data from police relating to taxis/PHVs.

Thought should therefore be given to what the particular vulnerabilities are in the local context, as authorities are used to doing in other areas of licensing, such as alcohol. For example, consideration could be given to the following:

- Is there significant use of taxis in the evening or late at night as part of the night-time economy? Both passengers and drivers could be increasingly vulnerable if passengers are under the influence of alcohol.
- Is there significant use of taxis by children and young people to/from school or activities? Again, concerns about vulnerability could be more prominent where lots of children/young people are relying on them for transportation.

15 More information about DPIAs can be found on ICOs website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments

16 www.gov.uk/government/publications/surveillance-camera-commissioners-buyerstoolkit

- Is there evidence of, statistics around crime involving PHVs/taxis, for example attacks on drivers?
- Is there evidence of complaints where the use of CCTV would have helped?

The DPIA also sets out measures that can be taken to mitigate any risks identified. It is important to note that where a DPIA identifies 'high risk' and there are not measures that can be taken to reduce this, authorities will need to consult the ICO before proceeding further. Ultimately this will help to inform the approach councils decide to take.

This is even more important if audio recording is being considered. As noted above, audio recording is regarded as more intrusive than video and therefore will need further justification. For example, an assessment might reveal that there are certain times when vulnerability is increased, such as in the early hours of the morning, and therefore there could be a strong argument for audio recording at these times, but not necessarily at others.

As the regulator, the ICO has successfully challenged councils on policies which they feel have not been justified, as in the Southampton case discussed in the next section. A robust assessment of necessity and risk through a DPIA and seeking legal advice could help avoid enforcement action by the ICO. In addition the SC Code is clear that mandating CCTV as a licensing condition will need a strong justification.

Consultation and engagement

Consultation and engagement are critical steps when considering deploying CCTV and even more critical when mandating its use and can help to shape the scope of the policy. The SCC's Passport to Compliance document includes sections on effective consultation in this area.

Consultation and engagement provides an opportunity to identify any concerns the public, the trade or other key stakeholders might have about proposals, these can then be addressed as proposals develop. Evidence of this process will be important to show how the licensing authority has had regard to balancing public protection and individual privacy, a necessary part of complying with the legislation.

Consultation and engagement with key stakeholders should be undertaken in line with your own council's consultation guidelines and it is an important step in the DPIA. A robust consultation process may help to avoid challenge further down the line. In Rotherham, the extensive consultation and engagement the council undertook was used as evidence when the council was legally challenged on their policy.

Key stakeholders are those who are most likely to be directly affected by the proposals, or groups representing their interests. These might include:

- Surveillance Camera Commissioner (Home Office) and Information Commissioner's Office
- councillors
- taxi/PHV trade bodies, operators and drivers
- residents
- specific taxi/PHV user groups
- suppliers of audio visual equipment
- local authority CCTV manager
- local police force.

Analysis of consultation responses will help to build an evidence base and identify the potential impact of mandating CCTV. Early engagement with the trade in particular is likely to be key to identifying what they see as the key issues and will give authorities the opportunity to shape a proposal which addresses any concerns. It is also important to have early discussions with the SCC and ICO.

Data protection, privacy and information governance

As discussed earlier it is important for councils to consider the potential impact of mandating CCTV on privacy and demonstrate through a DPIA that the approach to how/when CCTV systems are required to be used strikes a proportionate balance between privacy and safeguarding.

There are also steps that need to be taken to make sure that personal data which is being processed – which includes any visual or audio recording collected – is kept safe and secure. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) regulates the use of 'personal data' and licensing authorities will need to take steps to ensure a policy is developed that complies with GDPR and DPA to avoid any potential challenge or enforcement action. In practice this means that authorities need to think about data privacy from the outset, it should not be an afterthought.

The regulatory framework

There is a range of legislation and codes of practice around surveillance and data protection that are relevant for the use of CCTV systems in taxis/PHVs, these are set out in Appendix three. The Surveillance Camera Commissioner (SCC) and the Information Commissioner (ICO) both are the key regulators on the use of CCTV in taxis/PHVs.

Guidance from the Surveillance Camera Commissioner (SCC)

A good starting point when considering introducing a mandatory policy is the Surveillance Camera Code of Practice[17] (SC Code), which includes 12 guiding principles which should apply to all surveillance camera systems, including CCTV in taxis/PHVs. Local authorities have a statutory duty to 'pay due regard' to the SC Code under the Protection of Freedoms Act 2012.

In deciding to mandate CCTV systems and defining how they should be used, licensing authorities act as a 'system operator', and as such will need both to be aware of and adopt these principles.[18] In particular, principle one states that CCTV surveillance must be for a specific purpose, in pursuit of a legitimate aim and necessary to meet an identified pressing need. Policies should also be kept under review to ensure that the use of CCTV remains justified and proportionate and continues to meet its stated purpose (principles two and 10 of the SC Code refer to this).

There are several tools issued by the SSC which support authorities both to comply and demonstrate compliance with the SC Code. This includes the Passport to Compliance, which acts as a guide through the various questions that can be asked to help evidence that due regard has been paid to the impacts a policy will have and that risks identified have been mitigated.

17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

18 www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

The SCC's self-assessment tools[19] will also assist authorities to demonstrate publicly their compliance with the Code once CCTV is installed and operating. Councils can also apply for the Commissioner's third party certification mark, which demonstrates compliance with the SC Code.[20]

Failure to pay due regard to PoFA and the SC Code risks undermining the evidential integrity of any recordings derived from CCTV systems, should these need to be used as evidence in criminal or civil proceedings.[21]

Guidance from the Information Commissioner

Whilst the SCC regulates surveillance cameras, the Information Commissioner's Office (ICO) regulates personal data and is responsible for enforcing compliance with privacy and data protection legislation. The ICO has separate guidance and codes, such as the CCTV Code of Practice[22], to help organisations to comply with data protection legislation. The ICO's code does make reference to the SC Code and in complying with the SC Code authorities will have gone a long way to complying with the ICO's code already.

Given the ICO has challenged some of the authorities that have introduced mandatory policies it is recommended that authorities ensure they are fully compliant with both the DPA and PoFA. A summary of the key requirements is outlined in the following sections.

The ICO has been clear that if CCTV systems are to be mandated as part of the conditions of a licence, there will need to be a strong justification, and the policy must be reviewed regularly, especially where audio recording is being used in addition to cameras.

The law is clear that the use of CCTV and audio in taxis must be proportionate to the risk presented, and councils will need to set out a clear justification of why they believe there is a need for visual and audio recording if applicable. The main rationale for using audio recording in taxis/PHVs is that this would pick up any inappropriate conversations between passengers and drivers, for example when they are carrying children. Authorities will need to assess whether audio recording is necessary based on local circumstances, and be able to justify this.

As discussed earlier, authorities will be required to undertake a DPIA to demonstrate that the impact of CCTV systems in taxis/PHVs on privacy has been carefully thought through and the statutory obligations placed upon the council to comply with GDPR have been appropriately addressed. The ICO provide detailed guidance on DPIAs on their website[23] and the SCC has also issued a number of helpful tools.[24] The process of completing these assessments will also support councils in evaluating what a proportionate use of CCTV systems in taxis/PHVs might look like in the local context.

The ICO also encourages cameras be capable of providing a privacy friendly solution, for example where audio is used, both drivers and passengers should have independent controls for activating it. Once activated, authorities will need to consider how long audio recording should continue, and measures will need to be put in place to make sure recording is discontinued before other passengers enter the vehicle.

On the basis that there is adequate evidence and justification for a given approach, the ICO has in some cases taken the view that it is

19 They can be accessed by the following link: www.gov.uk/government/uploads/system/uploads/attachment_data/file/524525/Self_assessment_tool_v3_WEB_2016.pdf

20 www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme

21 Local authorities should note section 33(3) and 33(4) of PoFA – that the SC Code is admissible in evidence in criminal and civil proceedings and where the SC Code hasn't been given due regard a court or tribunal should take this into account. The CPS are updating their disclosure manual (September 2018) – the Surveillance Camera Commissioner has blogged about this: https://videosurveillance.blog.gov.uk/2018/07/17/disclosure-the-importance-of-complying-with-the-surveillance-camera-code-of-practice/

22 https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

23 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

24 www.gov.uk/government/organisations/surveillance-camera-commissioner

acceptable for cameras to be on permanently whilst the vehicle is being used for business purposes, but must be capable of being switched off when the vehicle is used in a private capacity. The Commissioner's blog details their position that where a taxi is being used by a driver for their own private or domestic purpose, continuous recording is likely to be unlawful, unfair and excessive under data protection legislation and in breach of Article 8 of the Human Rights Act 1998.[25]

The ICO's work on this is currently ongoing, particularly around the issue of continuous recording when the taxi is being used privately by the driver. To assist with this work, the ICO is engaging with a number of licensing authorities and further advice will be published by the ICO once this work has concluded.

When looking at what practical measures can be put in place to mitigate concerns around privacy, a robust download policy which clearly sets out the tightly-defined conditions/ circumstances under which footage can be downloaded from the CCTV system will be key. The policy should also demonstrate that any data held is kept securely and for a defined period of time in line with duties under GDPR.

Following guidance from the SCC and ICO and engaging with both organisations will help licensing authorities to balance privacy and safeguarding in a justifiable and proportionate way.

Rotherham Council's taxi camera policy

Suitable equipment, capable of recording both audio and video, must be installed in all licensed vehicles. The system must meet or exceed the council's specification for taxi camera systems and must be operational at all times that the vehicle is being used as a licensed vehicle (ie for the carriage of fare paying passengers). The system does not need to be operational during other times (for example when being used for domestic purposes).

Video recording must be active at all times. Audio recording must be active in any of the following circumstances:

- An unaccompanied child (ie under 18) or vulnerable adult is being carried in the vehicle.
- Where the driver and customer are involved in a dispute or the driver feels threatened by the behaviour of a passenger. Activation of audio recording must be triggered by the driver pressing a switch/button. Audio recording will continue until such time as the button/switch is pressed again. This switch will activate/deactivate audio recording independent of the passenger's audio activation button/switch.

There must also be the facility for the passenger to activate audio recording (independent of the driver) should the passenger wish to do so. Activation of audio recording must be triggered by the passenger pressing a switch/button. Audio recording will continue until such time as the button/switch is pressed again. This switch will activate/ deactivate audio recording independent of the driver's audio activation button/switch.

Once activated (by either passenger or driver), the audio recording must continue for an uninterrupted period until it is deactivated. There must be an indicator located within the vehicle that is clearly visible to the passenger and clearly shows that audio recording is taking place.

At the end of the journey when the passenger leaves the vehicle, audio must be deactivated before another passenger enters the vehicle. If appropriate it must be reactivated should any of the situations above arise in relation to this new journey.

Rotherham's policy was developed in view of the SC Code and ICOs code of practice and in consultation with both regulators.

Source: Hackney Carriage & Private Hire Licensing Policy (p.25)

www.rotherham.gov.uk/downloads/file/2473/rotherham_mbc_taxi_and_hackney_carriage_policy

25 https://ico.org.uk/about-the-ico/news-and-events/blog-continuous-cctv-in-taxis-where-do-councils-stand

Audio recording

The use of audio recording is considered more intrusive of privacy than cameras and requires strong justification. Where authorities opt to mandate audio recording, the justification for this will need to be clearly set out in the DPIA and the hours of operation of audio recording in particular should be considered carefully. The ICO's code includes a useful set of questions that must be thought through before audio recording is considered:

- Is there a pressing social need and do you have evidence that this need must be addressed?
- Have you considered other less privacy intrusive methods of addressing the need?
- Have the alternative options been reviewed and is there evidence to show that the only way to address the issue is through the use of audio recording?
- Have you got a clear specification for the audio system to ensure appropriate privacy and the necessary quality of recording?
- Is the public aware when audio recording is taking place, and how they can activate it?

In practical terms, the ICO has suggested that an audio recording system that allows recording to be switched on and off easily is a 'privacy friendly solution', as it does not require continuous recording and therefore mitigates the potential risk of recording excessive amounts of information. Again the local context will be important in determining what is appropriate.

Southampton Council's policy on the use of audio recording was challenged by the ICO for breaches of the Data Protection Act. The tribunal's view was that the requirement for continual 'blanket' audio recording in licensed vehicles was disproportionate, with the impact on the right of privacy outweighing any positive impact it may have on public safety or reducing crime. The tribunal's report can be read here: www.southampton.gov.uk/moderngov/documents/s18170/Appendix%204.pdf

As a result of this Southampton amended their requirements around audio recording and adopted a more targeted scheme. Southampton's policy sets out circumstances when audio recording should be activated based on times of day, types of customer (for example, children or vulnerable adults) and the use of panic buttons.

Similarly, Rossendale council's policy determines specific times when audio recording is required to be activated. This includes whenever an unaccompanied child (ie under 18) or vulnerable adult is being carried in the vehicle, or if there is a dispute with a passenger, or a driver feels threatened by a passenger's behaviour.

Information governance

Alongside considerations about when and what information should be captured, a key part of managing obligations under GDPR is what happens to the information captured. Information governance is the term used to describe the policies, procedures and processes implemented to manage information that is collected, in this case those visual and audio recordings captured by CCTV systems.

Councils polices therefore will need to cover how data is kept secure when it is held within a system in the vehicle, at the point of download, and once information is downloaded.

Who has responsibility for the control of data captured on CCTV systems?

In terms of who has responsibility for information captured by CCTV systems in taxis/PHVs, GDPR defines a data controller as the individual or organisation which has ultimate responsibility for how personal data is collected and processed.

The ICOs position is that in most circumstances it is the council which is the data controller, not an individual taxi driver and this position is set out in the Commissioner's blog post.[26] This is due to the fact that in mandating CCTV the council will usually be responsible for the purpose of the processing and defining how and when systems should be used, and how data is processed.

Data controllers are required to register with the ICO. In most cases councils will already be registered with the ICO as data controllers, but registration will need to be updated to reflect new use of personal data where a taxi/PHV CCTV policy is adopted. Authorities should engage with data protection officers within your own organisations to discuss this.

Where a council chooses to use a third party service provider as remote storage for taxi/PHV CCTV data, or to process or manage the CCTV data, the third party will act as a 'data processor'. A formal written contract is required between the data controller and data processor covering security arrangements, retention/deletion instructions, access requests and termination arrangements. For more information, the ICO has a detailed guide around the roles of data processors and data controllers: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts

As data controller the licensing authority is ultimately responsible for how images/recordings are stored and used, determining in what circumstances the images should be disclosed and for complying with all relevant data protection legislation. This can all be set out in a download policy, as set out in the next section.

Developing a data download policy

Licensing authorities will need to put in place clear policies around how information captured will be protected throughout its lifetime, ie from when it is recorded to when it is either downloaded or destroyed, this should be in the form of a download policy.

How CCTV systems capture and store information

When activated, cameras and audio equipment will record data which is automatically saved onto a memory recording system, like a memory card. The recording system and memory card (or other image memory recording system) are hardwired into the vehicle, and need to be securely stored within the vehicle, away from public access, and should be tamper proof.

Recordings should be stored on the internal memory for a defined period of time set out by the licensing authority, for example 31 days. After this period of time, unless there has been a request for download, the recordings should be over-written or destroyed.

The images contained in the recording device can only be downloaded by an authorised officer of the council or police officer. Where data is downloaded, there should be clear guidelines for how long this data is then be kept and how it is stored.

The ICO's code of practice sets out detailed information about how information should be stored, viewed and disclosed. This guidance is outlined briefly below, but councils are advised to read the code of practice in full.[27] Principles six, seven and nine of the SC Code also cover the storage and use of images captured from CCTV in taxis.

26 https://ico.org.uk/about-the-ico/news-and-events/blog-continuous-cctv-in-taxis-where-do-councils-stand

27 https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

For example, a download policy should set out clearly:

- that the licensing authority is responsible for the control of data captured by CCTV systems in taxis/PHVs
- how the information should be used and the circumstances in which it may be downloaded
- to whom it may be disclosed
- how long it should be kept for.

Recorded material should be stored in a way that maintains the integrity of the information so councils will need to ensure that the information is secure and where necessary, encrypted. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. The encryption of data needs to be considered both when it is 'at rest' and 'in transit', ie when the data is being moved from the recording device in the vehicle to another server.

CCTV systems should be installed in a way that allows data to be secured in a locked 'data box' inside a vehicle as well as being encrypted. Council's may want to consider compiling a list of permitted installers in the area so they can be confident that installation requirements have been met and data is secure.

Attention must also be given to the data that is downloaded and extracted. Councils will need to make provision for this data which is likely to involve separate storage arrangements, different retention periods and potentially different access controls. For example, when footage is captured on a device, it will usually be over-written after a given time period. However where footage is downloaded, for example to investigate an incident, this will be stored separately on a server for as long as is needed for investigation and possible prosecution purposes. This will generally need to be kept for longer than footage which is not accessed.

Integrity of images

Principle 11 of the SC Code relates to the importance of processing data in a way that retains its integrity (ie its accuracy and consistency) and this will need to be addressed in relation to the images/audio recordings captured by CCTV in taxis. This is of particular importance should any of this data be used as evidence for a prosecution in the criminal justice system.

It is important that there are effective safeguards in place to ensure the integrity of recorded images and information that is stored, so that it can be used for its intended purpose. For example ensuring that time, date and location of recordings (known as meta data) is recorded reliably, and that compression of data does not reduce its quality.

It is also important to ensure that data is recorded and stored in a format that allows it to be shared with ease with appropriate law enforcement agencies when relevant. If this cannot be readily achieved it may undermine the purpose of having CCTV in the first place. Data therefore needs to be in a format that is easily shared, that can be readily exported and then stored and analysed without any loss of its integrity. In particular:

- a system user should be able to export images and information from a surveillance camera system when requested by a law enforcement agency
- the export of images and information should be possible without interrupting the operation of the system
- the exported images and information should be in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency
- the exported images and information must preserve the quality.

Data retention

A download policy should set out how long data will be retained by the licensing team. This should cover the time that data needs to be kept for on the recording device within the vehicle, as well as how long the licensing authority will retain data in the event that it is downloaded. It is worth thinking through what the appropriate retention period might be for different scenarios. For example, downloading data as part of routine enforcement activity for the purpose of checking that the system is operating correctly will necessitate a shorter retention period than downloads relating to a serious incident.

Authorities will need to ensure that their information governance policies are updated to make reference to the CCTV data retention period and the rationale for it. Principle six of the SC Code covers the retention of images captured from CCTV in taxis setting out that images should not be retained for any longer than is absolutely necessary.

Dealing with requests for downloads

The majority of the time, data will be deleted or over written without the need to download it. However, there will be certain circumstances when data will need to be downloaded from the system, for example if an incident occurs or during enforcement inspections of vehicles.

As set out on page 17, a download policy should be developed to set out the prescribed circumstances in which data will be downloaded. The policy will also need to set out where, and by whom downloads can be undertaken. Most policies will specify that data downloads should be conducted in the presence of at least two relevant people, one of those being a member of council staff who has been trained in the download of data from the system, and in the requirements of the policy.

Downloads might ordinarily take place at a council facility, but may on occasion be at another location. This should be described in the download policy.

Procedures should be put in place to check that any request for data is in an appropriate format detailing the powers that allow the release of the data and providing all the information required to ensure the correct footage can be identified. The request for download must state the approximate time of the event/occurrence and only the timescale relevant to the specific incident will be downloaded, decrypted and thereafter stored.

It is also recommended that a dedicated computer should be used to facilitate downloads from data boxes, and where downloaded footage can be securely kept until it can be transferred onto a dedicated secure storage system held by the licensing team. A working copy can be produced and given to the requesting authority/subject or retained by the investigating officer. The ICO has published an information sharing code of practice and recommends that the data flows for this process be documented in the DPIA: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Whilst the amount of download requests will vary from authority to authority, the expectation is that the presence of CCTV should reduce the number of incidents in taxis/PHVs and that therefore requests for downloads should be a relatively infrequent occurrence.

Council enforcement officers will need to be able to use the system to access and extract information where disclosure is appropriate so consideration will need to be given to what additional training might be necessary.

Extract from Southampton Council's download policy

The policy outlines that data will only ever be downloaded on four occasions:

- 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, eg police or social services, that has a legitimate requirement to have access to the data requested to assist them in an investigation that involves a licensed vehicle or driver
- to fulfil a Subject Access Request that is compliant with the Data Protection Act.

Subject access requests

GDPR gives individuals certain rights over their personal data, including the right to access personal data, to know how their data is being used and to object to the way their data is used. Requests from passengers for a copy of footage/audio recordings is referred to as a Subject Access Request (SAR). The SC Code (principle four) sets out that there must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

Information for individuals about how they can request access to any recordings (personal data) captured by CCTV systems in taxis/PHVs will need to be provided, and a process for responding to requests set out.

Councils will need to put in place provisions for dealing with SARs and the circumstances in which these requests will be accepted or refused. Whether accepted or refused, SARs require a response within one month of receipt.

Third party requests

A third party request essentially captures any other requests, which can include members of the public making a complaint, and the police. There is a slightly different process for dealing with requests for downloads from third parties. Where information is requested by the police, for example if a passenger has made an accusation about a taxi/PHV driver, or a driver is making allegations of threatening behaviour against passengers this will need to be dealt with as a 'third party' request.

Once council officers are satisfied that the request is legitimate arrangements should be made with the owner of the licensed vehicle for the vehicle to attend the designated premises where a download can take place, for example a council facility. If it is not practical then a member of the licensing team should attend the location of the vehicle or data box to facilitate the download. It is good practice for any download to be carried out in the presence of at least two relevant people, which could be two members of the licensing team.

The council would need to consider the reasons a third party is requesting the information and then identify if they have a lawful basis to disclose it. However, the DPA 2018, similarly to the DPA 1998, provides an exemption that allows the disclosure of information for the prevention or detection of crime or the apprehension or prosecution of offenders (Schedule 2 Part 1 Section 2).

Privacy notices

Under GDPR, individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR.

Privacy notices are used to inform the public about the collection and use of their personal data. In terms of CCTV recording in taxis/PHVs, privacy notices will need to set out why camera/audio recording is being used, how long data will be kept for, who will be able to access it and how to make a compliant.

Privacy notices will need to be prescribed by the council. Under GDPR (article 13 and 14) certain information is required to be included in a privacy notice. These are the:

- name and contact details of the licensing authority
- contact details of the authority's data protection officer
- purpose of the processing
- lawful basis for the processing
- recipients or categories of recipients of the personal data
- retention periods for the personal data
- rights available to individuals in respect of the processing
- right to lodge a complaint with a supervisory authority.

More information is available on the ICO's website[28] and principle three of the SC Code also refers to the need for transparency in the use of surveillance cameras.

All of the above considerations are also addressed within principle nine of the SC Code which sets out the SCC's expectation that surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

28 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed

Implementation and enforcement

Having considered safeguarding and privacy issues, and consulted on proposals to implement a mandatory CCTV policy, licensing authorities will need to develop clear policies outlining the agreed approach to CCTV systems. These should set out expectations for how these will be used, and how non-compliance will be tackled.

What should be included in a licensing policy?

Councils will need to update their existing taxi/PHV licensing policy to include new provisions for CCTV systems. The LGA encourages all licensing authorities to have an overarching taxi/PHV policy, but where they do not, a standalone policy in relation to CCTV should be developed.

The key things to cover in a policy are:

- that a CCTV system must be installed in all licensed vehicles
- that CCTV systems must meet the council's prescribed specification
- when and how CCTV systems are to be used
- reference to how the system can be activated by drivers/passengers and that there must be an indication that audio recording is in use
- information about fair processing which should be included on notices in vehicles with further information available on the council's website
- implementation timescales for new provisions
- that the system complies with relevant legislation.

Details of the system specification and implementation schedule can be provided as supplementary documents. Licensing authorities will need to ensure corporate information governance policies are also updated to include the use of CCTV data in taxis/PHVs.

Conditions of authority's taxi/PHV driver and vehicle licences will also need to be updated to reflect new requirements for CCTV.

Camera specification and installation

Principle eight of the SC Code of practice is clear that councils, as surveillance camera operators, should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards – there are a list of recommended standards on the SCC website.[29] It is up to individual councils to decide the extent to which they prescribe exactly what a CCTV system will need to do, but it is helpful to have a minimum standard which cameras/audio need to meet so drivers are clear about the requirements that systems need to meet. This will act as a guide for drivers when they are purchasing cameras.

Again, the SCC's Buyers' Toolkit and the Passport to Compliance documents will also provide a good guide when considering specifications.

29 www.gov.uk/guidance/recommended-standards-for-the-cctv-industry

Systems should also comply with relevant legislation and standards. Council's should satisfy themselves that the supplier is able to provide the relevant technical files for the entire system, including any ancillary equipment, and that the product is either CE or E marked if type approved. Test certificates provided by the manufacturer, particularly if outside of the EU, may not be sufficient for this purpose.

Clearly the cost of CCTV systems will depend on the specification a council has agreed and consideration should be given to how requirements can be balanced against the cost to drivers. In Rotherham, the taxi trade argued that the cost of systems that met the specification were too high and that this should be picked up by the council. However, the council considered that the systems represented a reasonable and legitimate business cost and noted the ability for the driver to offset costs. Elsewhere, some local authorities have identified funds to support drivers with the cost of installing systems.

The specification for CCTV systems will need to be set out either within a policy or as a separate annex. It is also helpful to set out a list of systems which meet the requirements of the policy and where these can be purchased. This may require some initial scoping work to ensure cameras that meet requirements are readily available and suppliers are able to meet the demand of the fleet size.

Installation of systems should be done by an installer approved by the local authority so that cameras/audio equipment are safe and secure. Including a list of approved local installers is one way to ensure this happens.

Communicating changes to drivers and members of the public

Using an effective communication strategy to raise awareness of the introduction of mandatory CCTV is important and there should be a proactive effort to make sure both drivers and operators, as well as the public are clear on exactly what the changes are, and the implications of these. Whilst drivers should already be aware of plans following earlier consultation, it is important that rules, policies and procedures are put in place ahead of implementation, and that all licensed drivers are informed, for example by letter, to ensure they fully understand the requirements that they will need to comply with. This should also give them an opportunity to prepare and budget for new requirements. Training could be offered to drivers around their responsibilities and how to deal with questions from passengers.

The public should also be informed about new proposals for example via press releases and other routine communications. To comply with data protection legislation and PoFA, all vehicles with CCTV systems fitted will need clear signage to let the public know that they are being recorded, and how they can find out more information, or make a request for a data download. The forms of this signage should be prescribed in your download policy. Detailed information should also be published on the council's website, and reviewed at least annually.

Implementation schedule

Developing and publishing an implementation plan is important and shows that new requirements are being introduced fairly and in a way that minimises the impact of potentially costly changes on the licensed trade.

Once a policy has been approved, it may be fair to say that requirements will have immediate effect in relation to new applications. Thought should be given to what a reasonable amount of time to install cameras in existing licenced vehicles would be and whether any exemptions might be appropriate, for example if vehicles are in their last year of operation due to age limit requirements.

One possible approach could be that vehicles with existing licenses are required to be fitted with CCTV within a defined amount of time, eg 18 months from the policy go live date or alternatively, there could be a requirement for vehicles to have CCTV installed at point of renewal following the go live date. Enforcement officers can then check that systems are installed correctly and working properly as part of the renewal process.

Adopting this type of staged approach will help to reduce the impact on CCTV system suppliers and installers, and also ensure that licence holders have sufficient time to source, purchase and install a system prior to the requirement taking effect.

Enforcement

The effectiveness of CCTV as a measure to improve safeguarding is reliant on enforcement activity to identify those who are not complying with the agreed policy, for example by not switching the systems on when they should be. If there is evidence that cameras are not being used in the agreed manner, steps will need to be taken to address this, in line with those set out in the council's policy.

The functionality of CCTV systems should be checked as part of routine enforcement activity although no one but the relevant council officer or where applicable authorised staff from the data processor should be able to access this data. In a similar way to how footage from CCTV systems in licensed premises is checked, a designated officer will need to check that the camera and audio functions are being used in line with local requirements. Officers will therefore need to be trained in functionality of the systems which meet the specification. It is worth considering what training needs will be required at the outset so that resources can be allocated to make sure officers have relevant training. Principle 11 of the SC Code covers this point.

Reviewing CCTV policies

Principles two and 10 of the SC Code set out that there should be regular reviews of CCTV systems to ensure that their use remains justified and proportionate in meeting its stated purpose.

By regularly checking CCTV systems you can make sure the cameras are working correctly, that footage can be downloaded correctly and so on. It is best practice to carry out reviews at least annually and this can be done for every camera or the entire system. The Surveillance Camera Commissioner's self-assessment tool is useful when carrying out a review and it is best practice for the outcome of the review to be published.

Appendices

Appendix 1: Flow chart

Planning and Feasibility

Why you want the system
Evidence of incidents relating to taxis/PHVs in the locality, concerns about CSE.

What you want it to do
Record images, audio recording.

Data protection impact assessment
How can you mitigate privacy concerns.

Developing a policy

Requirements for operation
When are cameras/ audio required to be in use, does the policy cover taxis and PHVs.

Data protection considerations
Who is the data controller, in what circumstances can data be downloaded, what is the retention period.

Protection of Freedoms considerations
Have you complied with PoFA and the SC Code.

Develop a technical specification
Including technical requirements and how systems should be installed, how data is kept secure.

Consultation
Full public consultation to seek views, this should inform the final policy which is taken to committee/ council for a decision.

Implementation/roll-out

Communications
With drivers, passengers and the general public about the new policy and where concerns can be directed.

Training
For council enforcement officers as well as for drivers about their responsibilities and how to deal with questions from passengers.

Implementation plan
Outline the approach to the roll out, and when licenced vehicles are expected to comply by.

Review
On-going review of the policy.

Appendix 2: Glossary

Surveillance camera systems
The statutory definition for a surveillance camera systems is set out in Section 29(6) of the 2012 Act[30] and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c).

A system operator is the person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.

A system user is a person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.

Date protection impact assessments (DPIA)
A data protection impact assessment (DPIA) is a process which helps to identify and minimise the data protection risks of a project. Under GDPR, a DPIA is required to be undertaken for 'high risk' processing which includes mandatory CCTV in taxis.

The DPIA will need to outline the purpose of the processing, assess the necessity and proportionality of a specified approach, as well as assess the potential risks to individuals and how these could be mitigated.

Data controller
A data controller determines the purposes and means of processing personal data.

Data processor
A processor is responsible for processing personal data on behalf of a controller

Data protection officer (DPOs)
DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding data protection impact assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. All public authorities are required to have one.

30 The Protection of Freedoms Act 2012 (PoFA) www.legislation.gov.uk/ukpga/2012/9/part/2

Appendix 3: Links to useful resources and guidance

Information Commissioner's Office

Guidance on Data Protection Impact Assessments
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Blog: 'Continuous CCTV in taxis – where do councils stand?'
https://ico.org.uk/about-the-ico/news-and-events/blog-continuous-cctv-in-taxis-where-do-councils-stand

Data protection code of practice for surveillance cameras and personal information
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Guidance on the role of data controllers and processors
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Individual rights
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Surveillance Camera Commissioner

Surveillance Camera Code of Practice
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

Passport to compliance: these documents will guide authorities through the relevant principles within the Surveillance Camera Code of Practice. It sets out the necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the code.
www.gov.uk/government/publications/passport-to-compliance

Self-assessment tool
www.gov.uk/government/uploads/system/uploads/attachment_data/file/524525/Self_assessment_tool_v3_WEB_2016.pdf

Third party certification
www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme

Buyers' Toolkit
An easy-to-follow guide for non-experts who are thinking about buying a surveillance camera system and want to ensure they buy an effective system that does what they want it to do.
www.gov.uk/government/publications/surveillance-camera-commissioners-buyers-toolkit

Blog 'CCTV in Taxis – are you taking to me?'
https://videosurveillance.blog.gov.uk/2018/08/28/cctv-in-taxis-are-you-talking-to-me/

Speech to the National Association of Taxi Drivers
www.gov.uk/government/speeches/surveillance-camera-commissioners-speech-to-the-national-taxi-association-agm

Useful case studies from the Commissioner
www.gov.uk/government/collections/surveillance-camera-code-of-practice-case-studies

Local Government Association
18 Smith Square
London SW1P 3HZ

Telephone 020 7664 3000
Fax 020 7664 3030
Email info@local.gov.uk
www.local.gov.uk

For a copy in Braille, larger print or audio,
please contact us on 020 7664 3000.
We consider requests on an individual basis.

REF 5.42