



## Privacy impact assessment for camera recording system (CCTV)

Use this template to record the PIA process and results. You should start to fill in details from the beginning of a project and amend the answers as you make progress with your business case. Keep a record of each draft of your PIA.

Please inform the Data Protection Officer if you amend your PIA after your business case has been approved.

### Summary information about the system

	<b>Name of system</b>	CCTV (in taxis and PHV's) Full name TBA
	<b>Summary of objective and background</b> (the PIA will ask for a more detailed description later in the form)	The mandatory introduction and installation of a standard, secure CCTV system in all Guildford Licenced vehicles, installation could begin in 2021.  The system will be GDPR compliant.
	<b>Relationships</b> For example, with other services, Local Authorities or organisations	Funding application from PCC submitted. Support investigations by Surrey Police and other statutory bodies.
	<b>Cross reference to other projects</b>	
	<b>Project Manager (where relevant)</b>	Mike Smith
	<b>Name and job title of Information Asset Owner</b> (see CCTV authorisation procedure rules)	Justine Fuller

## Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

**Describe the established and proper legal basis for the scheme.** For example, it would not be appropriate for the Council to use CCTV to investigate a matter that is not within its legal powers to investigate (e.g. a police matter or an issue where enforcement powers lie with another organisation).

Licensing authorities must consider as full a range of information available to them when making a decision whether to grant a licence and to meet their ongoing obligation to ensure a licensee remains suitable to hold a licence. The use of CCTV in all vehicles will provide increased level safety for the public and the driver. The use of the system will allow the authority to fulfil its statutory obligations to public safety and other agencies to lawfully access evidence.

The Policing and Crime Act 2017 enables the Secretary of State for Transport to issue statutory guidance on exercising taxi and private hire vehicle licensing functions to protect children and vulnerable individuals who are over 18 from harm when using these services.

**How will you make sure that the people recorded are aware that it is happening?**

All passengers must be made fully aware if CCTV is operating in a vehicle. Given that audio recording is considered to be more privacy intrusive, it is important that individuals are fully aware.

The system will offer continuous visual recording upon ignition, but there will be an option to turn this off by the driver should the vehicle be used for personal use. Audio recording will only be activated upon the driver/passenger pressing a button. Data will be stored on a secure encrypted hard drive which only GBC has access to upon request. The spec should you need it is in the draft policy document at:

<https://www.guildford.gov.uk/taxipolicy>

As well as clear signage in vehicles, information on booking systems will be introduced. This maybe text on a website, scripts or automated messages on telephone systems.

**Why is the scheme necessary to address a pressing need (such as public safety or crime prevention)?**

The use of CCTV in all vehicles will provide increased level of confidence and safety for the public and the driver.

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.

**Explain how the CCTV is justified and proportionate in the circumstances.**

Following high profile incidents involving offences committed by licenced drivers which impacted on the confidence of the public to use public transport the use of CCTV is an effective tool to increase safety for all, 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.

The Hackney Carriage and Private Hire trades have raised the issues of violence and theft against drivers in meetings of the trade working group.

Licensing Services already encourages self-reporting of incidents by passengers and drivers, with all complaints investigated. Surveillance camera footage will assist in making accurate and fair licensing decisions. There have been several occasions when investigating complaints where surveillance camera footage would have assisted, due to conflicting accounts.

Surveillance cameras can help deter crime, but also provide evidence of crimes which can be used by the police to apprehend perpetrators and used in court to achieve successful prosecutions.

The deterrence of crime is the primary objective of this project, particularly to safeguard vulnerable passengers and reassure drivers.

**What problems might arise from use of the proposed CCTV scheme?**

Concerns of the public that the authorities are spying on the public. The concern that the unlawful misuse of the data and who has access. 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.

**Explain what less privacy-intrusive solutions (for example, improved lighting) you have considered and why you think they will not be able to achieve the same objectives.**

The use of CCTV provides increase levels of confidence for both the driver and passenger. The use of CCTV has been shown to significantly impact on crime levels on public transport and offers authorities to obtain evidence of both crimes and conduct which is compelling.

Expand on the information you provided in the summary, covering:

- what the project aims to achieve – for example, public safety and security or staff monitoring and training or traffic flow monitoring or prevention and detection of crime and so on.
- Describe what quality is required. For example: Detecting presence (i.e. whether a person is present in an image without the need to see their face), Recognising (to recognise someone who is known or to determine that someone is NOT known), Identifying (to record high quality facial images that could be used in court to prove someone's identity beyond reasonable doubt)
- what the benefits will be to the organization and any other parties

Feel free to cross reference to other documents related to the project such as the Project Initiation Document and any reports to Corporate Management Team and Committees, which might record manager support for the proposal. But you should ensure any such documents are attached or linked to this PIA.

The system will record internal video footage of the driver and any passengers in the vehicle when the vehicle is being used as for private hire or hackney carriage use. Passengers can be anybody, including children or vulnerable groups.

Audio recording is not normally recorded, but recording will depending on the system selected be triggered by:

- Passengers' panic button
- Driver's panic button
- G-force sensor indicating a crash
- Shouting detected by a microphone
- Door opening when vehicle is in motion

## Part 2: Describe the information flows

Ideally you should map the system to explain how the information flows into, within and out of it.

Show the following

- What will be recorded?
- Where will the recordings take place? For example, how many cameras are involved, where will they be located and where will they feed to in order to store the recordings?
- What services, contractors, service partners, third parties and so on will have routine access to the system and its recordings?
- What disclosures will be made from the system and in what circumstances?
- What will be the routine retention period for recordings of incidents?
- You should give an indication of the scale of the surveillance – such as the number of individuals likely to be affected, where known.

Licensing Services will be the primary user of the data, however it is likely that the police will request data to assist with their investigations as well.

Other requests are expected from:

- Other licensing authorities – to make a licensing decision on a licensed driver or vehicle proprietor
- Motor insurance companies – to investigate claims made by the driver, vehicle proprietor or other drivers involved in an accident with the vehicle

When data is shared this is normally via:

- Secure email
- Encrypted email
- Encrypted data drive
- Disc, transferred directly between officers from the organisations



### Part 3: Consultation

<b>Stakeholders to be consulted</b>		
You should consider in detail what the interests of the various stakeholders are and the level of involvement they will have in the PIA.		
Do not list stakeholders if they are already part of your project team or a separate PIA team.		
<b>Stakeholder: Name/organisation/role</b>	<b>What interests do they have in the proposal?</b>	<b>How are you going to consult with them?</b>
Surveillance Camera Commissioner (Home Office) and Information Commissioner's Office	Regulatory body	Online consultation
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.	Online consultation Reports to committee
Taxi/PHV trade bodies, operators and drivers	Providers of service	Online consultation TAG Meetings
Residents	User of the service	Online consultation
Taxi/PHV user groups	As above	Online consultation
Suppliers of audio visual equipment	Suppliers of equipment	Tendering process
CCTV manager	User of information	Online consultation
Surrey Police	Investigation	Online consultation
SCC	User	Online consultation

### Consultation Plan

**Note:** If there is already a consultation strategy or plan in place for the project, you don't need to have a separate one for this PIA. You do, however, need to make sure that any consultation encompasses all the privacy aspects of the project.

Explain below what approach you are taking to consultation.

How will the results of the consultation be analysed and used to influence the CCTV project?

Consultation process was conducted in 2020 and the results are available for review.

### What could be done to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

Audio recording is disabled by default, but a five-minute recording could/will be triggered by:

- Passengers' panic button
- Driver's panic button
- Shouting detected by a microphone
- Door opening when vehicle is in motion

An audible warning and visual light shall indicate when audio recording is occurring.

Full specification pending once supplier formally selected.



**Part 5: Approval and integration of the PIA outcomes back into the project plan or the ongoing management of the process or system**

Who is responsible for putting in place the solutions that have been approved?

Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns (post title with responsibility)

TBA

**Approval for the PIA**

Name	
Post title	
Responsibility in relation to the project	
Signature	
Date of approval	
Planned date of next review of PIA	

**Consider how the recordings will be managed in a way to minimise any unwarranted impact on the privacy of those recorded (for example, storage of data, destruction of data).**

Explain

**Explain the arrangements you have put in place to review the CCTV to ensure it continues to meet its stated purpose and is still necessary and proportionate.**

Explain

**Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely and in accordance with your procedures?

Will someone (other than Council employees) be using or storing information on behalf of the Council? If so, have they provided an information security guarantee and is the arrangement formalised by a written contract, which restricts the service provider to acting only on the instructions of the Council?

## Annex 4

### Information Security and Technical Considerations

#### Part 2 Privacy Impact Assessment Key questions

<p><b>Who will have access to the information held or produced by the asset?</b></p>	<p>Licensing Services will be the primary user of the data, however it is likely that the police will request data to assist with their investigations as well.</p> <p>Other requests are expected from:</p> <ul style="list-style-type: none"> <li>• Other licensing authorities – to make a licensing decision on a licensed driver or vehicle proprietor</li> <li>• Motor insurance companies – to investigate claims made by the driver, vehicle proprietor or other drivers involved in an accident with the vehicle</li> </ul>
<p><b>Is there a useable audit trail in place for the asset. For example to identify who has accessed recorded or live footage? Please describe it in detail</b></p>	<p>Footage will be retrieved by an authorised officer in the course of investigating a complaint or crime. Depending on the solution procured, this may be via physical or remote connection.</p>
<p><b>How and where will the information be kept, stored, accessed?</b></p>	<p>On a database</p>
<p><b>Will any information be sent or hosted off-site?</b></p> <p><b>If yes where?</b></p>	<p>No</p>
<p><b>Please state by which method the information will be transported</b></p>	<p>Encrypted email GSx Mail By hand</p>
<p><b>Does this arrangement include any of the following being carried out, on behalf of the Council, by any other organisation, person or individual (not directly employed by the Council)</b></p> <p>If you answer “yes” to any of these you must make sure they have provided a sufficient security guarantee and that the arrangement is under a written contract under which the data processor is to act only on the instructions of the Council</p>	<ul style="list-style-type: none"> <li>• Obtaining personal data</li> <li>• Recording personal data</li> <li>• Holding (or hosting) personal data</li> <li>• Organisation, adaption or alteration of personal data</li> <li>• Retrieval, consultation or use of the information or data</li> <li>• Disclosure of the information or otherwise making it available</li> <li>• Alignment, combination, blocking, erasure or destruction of personal data</li> </ul>

	<b>See Appendix 5 for the data processor security questionnaire</b>	
	<b>Is the PIA approved? If not, please state why and set out the improvement plan required to ensure the PIA can be approved</b>	Yes  No

## Annex 5

### Information Security Considerations in respect of data processors\*

\*A data processor is anyone who will do any of the following on behalf of the Council:

- Obtaining personal data
- Recording personal data
- Holding or hosting personal data
- Carrying out any operation or set of operations on the information or data
- Organisation, adaption or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure, dissemination or otherwise making information or data available
- Alignment, combination, blocking, erasure or destruction of personal data

## SERVICE PROVIDER'S INFORMATION SECURITY

**Name of service provider or organisation:**

---

**Description of Service to be provided or name of contract:**

(For example, what categories of personal information will be processed\* on behalf of Guildford Borough Council and how?)

---

Please note that asterisked items (\*) are not applicable to sole traders.

### ORGANISATIONAL SECURITY

	Measures	Tick as appropriate	Details, where required
1.	Has the service provider appointed an individual to take control of data protection responsibilities?  If so, please provide the name and contact details		
2. *	Has the service provider implemented a Data Protection Policy?  If so, please return a copy with this questionnaire.		
3.	Has the service provider achieved certification as complying with any recognised national or international standards relating to information security		

	Measures	Tick as appropriate	Details, where required
	(such as ISO27001)?  If so, please provide evidence of certification		
4	Has the service provider passed a recent audit relating to information governance standards?  If so, please provide evidence, such as an executive summary of the audit report.		
5	Will a sub contractor have access to the Council's personal information?  If so please provide identify the sub-contractor(s)		
6	If the answer to the above was 'Yes', please describe what processing the sub contractor will be carrying out (e.g. hosting a database)		
7	Please provide detailed evidence to show the extent to which the sub contractor's security arrangements have been vetted to ensure they are at least the same as the contractor's		
8	Does the service provider work to or comply any regulations or codes of practice relevant to the use of personal information?  Please describe (For example, the Market Research Society Code of Conduct, PCI Security Standards and so on)		
4.	How does the service provider vet and train their staff and subcontractors, who will have access to the Council's personal information,  Please provide details of vetting and training procedures: service provider and sub contractors		
5.	Does the Service Provider treat any breach of their data protection policy and procedures as a disciplinary offence?  Please provide evidence, for example, the relevant wording included in employment contracts.		

	Measures	Tick as appropriate	Details, where required
6.	<p>What controls are in place to restrict access to the personal information to authorised people only?</p> <p>Please briefly describe</p> <p><i>(Sole traders or organisations which make use of home facilities should indicate measures taken to ensure unauthorised access to the information does not occur at home)</i></p>		
7.	<p>Does the service provider have provisions in place with their sub contractors to ensure similar levels of protection can be guaranteed if the subcontractor has access to the personal information?</p> <p><i>Note: this is relevant only if the contract allows the service provider to employ a sub-contractor</i></p>		

### TECHNICAL SECURITY

	Measures	Description
1	Location of servers, which will host the data?	

2.	<p>Describe the technical measures restricting access to systems holding personal data</p> <p><b>Minimum standards</b>  If customers enter or access their own personal data (e.g. to access their account), the connection must be via https:// and require a complex password)</p> <p>If the system will be hosted outside of the Council's network and protectively marked information can be accessed remotely e.g. via the internet, the minimum security standard is two-factor authentication (for example, complex password in addition to a soft token or biometrics or IP address restriction)</p>	
3.	<p>If the service provider will host a system remotely, how will access be restricted in the event of a member of staff leaving the Council's employment at short notice?</p>	
4.	<p>What technical measures in place to secure personal information when in transit?</p> <p>If protectively marked information will be transferred, the data must be encrypted</p>	
5.	<p>If automated systems are to be provided, describe the security measures in place</p> <p>(bear in mind that sensitive personal data will require more stringent security than other kinds of information)</p>	
6.	<p>Is the personal information backed up on a daily basis and stored in a secure site?</p>	
7.	<p>When was the last penetration testing carried out on the system and what was the result?</p>	
8.	<p>If protectively marked information is involved, describe how access to it will be audited or recorded so that breach allegations can be investigated</p>	



## PHYSICAL SECURITY

	Measures	Tick as appropriate	Description, where required
1	Are the premises on which the personal information is to be stored secure?		
2	Is access to those premises restricted?		
3	Are the premises subject to 24-hour security?  Please describe (eg CCTV, security guards etc)		
4	Describe the access restrictions in place for non-automated information (e.g. paper files, discs, microfilm and microfiche)  (eg, lockable filing cabinets, clear desk policies etc)		
5	Are any copies of the personal information, printouts, obsolete back-up tapes etc, disposed of securely?  Please describe		
6	Is obsolete hardware and software from which the information could be recovered disposed of securely?  Please describe		
7	Does the service provider have an auditable retention and destruction policy?  Please return a copy of the policy with this questionnaire		

## LOCATION AND LEGISLATION

	Measures	Tick as appropriate	Description, where required
1	Will the information be stored on servers outside of the European Economic Area		

	(EEA)?		
2	Will the Service Provider confirm that they will comply with the General Data Protection Regulation?		

Guildford Borough Council reserves the right to audit the service provider to monitor compliance unless the service provider can provide evidence of having successfully passed a data protection audit provided by a reputable third party assessment body.

---

I certify as an authorised representative of the service provider that the answers to the above questions are true and guarantee that any measures indicated will be applied to any personal information used on behalf of Guildford Borough Council for the purposes of this agreement.

PRINT NAME:

POSITION:

NAME OF SERVICE PROVIDER OR ORGANISATION:

SIGNATURE:

DATE:

**\*DEFINITIONS:**

**“Personal data” (“personal information”):** data relating to a living individual who can be identified...including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

**“Processing”** includes any of the following activities: Obtaining, Recording, Holding information, Carrying out any operation on the information, Organisation, Adaption, Alteration, Retrieval, Consultation, Use, Disclosure by transmission, dissemination or otherwise making available, Alignment, combination, blocking, Erasure or destruction of information or data