Data Protection Impact Assessment

Project Details

Name of Project
Taxi Cameras
Brief Summary of Project
To require licensed hackney carriages and private hire vehicles to have fitted an approved taxi camera system.
Estimated Completion Date
On going
Name of Project Lead
Phil Bates

Details of Person Conducting DPIA

Name
Phil Bates
Position
Service Manager Licensing
Contact Email Address
Phil.bates@southampton.gov.uk

Step 1: Identifying the need for a DPIA

Does your project involve the processing of personal data by or on behalf of Southampton City Council?
"Personal Data" means information that relates to an individual, who can be identified (either by the information alone, or when combined with other information). "Processing" means collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, combining, restricting, erasing or destroying. It should be integral to the project, and not just incidental to it.
☒ Yes ☐ No
If your project does **not** involve the processing of personal data by or on behalf of Southampton City Council, tick the declaration at the end of this section. If your project **does** involve the processing of personal data by or on behalf of Southampton City Council, proceed to the next set of screening questions below.

Does your project involve any of the following? (Not all may apply, tick those that do)
☒ The collection of new information about individuals
☒ Compelling individuals to provide information about themselves
☐ The disclosure of information about individuals to organisations or people who have not previously had routine access to the information
☐ The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used
☐ Contacting individuals in ways which they may find intrusive
☐ Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held

Are you planning to carry out any of the following? (Not all may apply, tick those that do)
☐ Evaluation or scoring
☐ Processing of sensitive data or data of a highly personal nature
☒ Processing on a large scale[1]
☒ Processing of data concerning vulnerable data subjects
☐ Processing that involves preventing data subjects from exercising a right or using a service or contract

Do you plan to…? (Not all may apply, tick those that do)
☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people
☐ Process special-category data[2] or criminal-offence data on a large scale
☐ Systematically monitor a publicly accessible place on a large scale
☐ Use innovative technological or organisational solutions
☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
☐ Carry out profiling on a large scale
☐ Process biometric or genetic data
☐ Combine, compare or match data from multiple sources
☐ Process personal data without providing a privacy notice directly to the individual
☐ Process personal data in a way that involves tracking individuals' online or offline location or behaviour
☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
☐ Process personal data that could result in a risk of physical harm in the event of a security breach

[1] "Large scale" can mean the number of individuals involved, the volume of data, the variety of data, the duration of processing, or geographical area.
[2] Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

If you have ticked any of these, please proceed to Step 2.
If **none** of these apply, please tick the below box, and return the form to the Information Lawyer (Data Protection Officer) at dataprotection@southampton.gov.uk
☐ None of the screening statements in Step 1 of this document apply to the project, and I have determined that it is not necessary to conduct a Data Protection Impact Assessment

Step 2: Describe the processing

Details of the Personal Data
What type of personal data is being processed? Tick all that apply
☐ Education and training details ☐ Employment details ☐ Family, lifestyle and social circumstances ☐ Financial details ☐ Goods or services provided and related information ☐ Personal details issued as an identifier (e.g. NHS Number) ☒ Personal details, including any information that identifies the data subject and their personal characteristics
What is the nature of the data?
INFO: Detail the type of personal data being processed. List any fields that will be processed (e.g. name, address, data of birth, NHS number, video images)
Visual data (video) of individuals inside of a licensed hackney carriage or private hire vehicle. Audio data of conversations will also be collected on activation of a panic button by the driver.
What special category / sensitive data is being processed? Tick all that apply
☒ Physical or mental health ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sexual orientation ☐ Criminal record ☐ Criminal proceedings ☒ Racial or ethnic origin ☐ Political opinions ☐ Biometric or Genetic data ☐ No special category / sensitive data

What is the nature of the special category / sensitive data? Please provide further information
Visual data of the subjects and conversations if the audio data is activated. The recording of audio data when triggered may collect data as to the commission of criminal offences. In very limited cases, the actions of the individuals may lead to special category data being captured but will normally be incidental and inferred by their actions or comments. Unless the criminal offence or special category data is relevant to the purpose of the disclosure, the data will not be used and in the vast majority of cases will not be accessed.
Does the project involve the use of social care data?
☐ Yes ☒ No
Does the project utilise existing and established IT systems, or require the use / procurement of a new system?
☒ Existing / established system ☐ New system

The nature of the processing

Briefly describe the flow of personal data

INFO: Describe “the journey” of the data, from the point of collection from the data subject, through the various parties and departments involved.

As per the Taxi Camera Policy, visual data capture is triggered by the ignition of the vehicle being turned on and goes off 20 minutes after the ignition is turned off.

Audio data is triggered for five minutes by the driver pressing a button. All the data is held on an encrypted drive or solid-state card separate from the camera head in a secured position within the vehicle.

Should the criteria be met to download the data is transferred from the card / drive to a standalone laptop with the appropriate encryption software.

The data is then transferred to a hard drive and then either to a DVD or securely uploaded to the requester’s servers. Uploading data will only sent to enforcement agencies, such as the police or government departments entitled to the data. The card / drive is returned to the vehicle and data overwrites once the storge is full. The data on the laptop is deleted, the hard drive is kept in a locked safe and the DVD is kept in a secure cupboard within the office as a working copy or until handed to the requestor.

Except for holding data for the purposes of viewing at court or as a part of an investigation data is not held directly on the laptops but instead within SCC servers. Very little data is held in this manner and access is restricted to licensing staff and some IT staff for IT maintenance purposes.

The servers have either McAfee Drive Encryption or moving forward Microsoft Bitlocker. There is no encryption on the hard drive, but this is locked in a safe that is bolted to the ground and kept within the licensing office. Licensing do not share the office with any other department. Laptops are password protected.

How will the data be collected? E.g. via form, system transfer, face to face etc.

Visual images of inside licensed vehicles will be recorded once the ignition is turned on and up to 20 minutes after the ignition is turned off. Generally, the images will show the front passenger and driver from the chest upwards, depending on the seating, images of passengers in the rear seats will show them from the waist upwards.

Audio recording will be triggered for a period of 5 minutes on the pressing of a button accessible to the driver. The audio recordings will capture any conversation within the vehicle, including driver and passengers. It does collect noise from outside of the vehicle when the windows are open and only conversations outside of the car that occur directly by an opened window will be heard.

The data is stored on either a hard drive or sim card which is separate from the camera head behind a lock and the data is encrypted to government recommended standards, 256-bit encryption. The storage component should be capable of storing a minimum of 168 hours of data and to overwrite data automatically once the memory is full.

How will the data be used?
Vast majority of data will not be used or even seen / heard, whether by the driver, passengers, Council officers, or anyone else. This is because the data is stored in encrypted form in a recording device within the vehicle. The taxi camera policy contains the criteria when a data from a taxi camera can be downloaded (which sets out when data will be decrypted, downloaded and used. This policy is regularly reviewed, with the last review taking place in August 2022. The purpose of the scheme is to protect both public and drivers and to give the public confidence that using taxis is a safe option. The policy allows for downloads to occur to assist in the investigation of a crime, a complaint related to taxi licensing, legitimate requests from an authority with an investigation linked to a licensed vehicle or driver and subject access requests. Only approved members of the licensing team can undertake the downloads and as such normally determine if such a request fits the criteria, any doubtful ones are either referred to the manager or the Data Protection Officer for guidance. Once the data is retrieved from the hard drive it is kept secure within the office. The data is either handed to the requestor, normally a police officer, or the investigating officer for complaints. Historically, public have complained of sexual assault and inappropriate behavior by drivers. There is often little to no corroboration for these incidents, the cameras and audio recordings assist in providing corroboration. This empowers victims to make statements as they know there will be a good chance of corroborating evidence from the camera, increases the chances of a successful prosecutions, provides key evidence for determining bodies assessing the fitness and propriety of drivers and act as a deterrent to would be offenders. Drivers have been victims of serious assaults and abuse including racial abuse, again the cameras and audio recordings assist in providing the corroborative evidence required for relevant authorities to take action. They also protect innocent drivers from false allegations. Since the implementation of the cameras, police investigating serious crimes such as murder, drugs and trafficking offences have sought data from the cameras as it is clear individuals involved in such activity often resort to licensed vehicles as a mode of transport. This evidence is assisting in linking individuals to phones linked to organized crime networks.
How will the data be stored?
Data is stored on a secure and encrypted hard drive within the vehicle. Any data downloaded will be copied onto a DVD and kept in a secure cabinet locked within the licensing office, only the licensing team will have access to this cabinet. The camera specification requires the storage device to be separate from the camera head and out of direct view. The encryption required has to meet FIPS 140(2) standard and more recently AES256 or equivalent.

These are the recommended levels of encryption for such data and would require a very high level of sophistication to breach.

A master copy of any downloaded material is retained for a period of one year on a standalone hard drive which is kept in a locked safe in the licensing office. This is in case the working copy gets corrupted.

Often the evidence recovered becomes evidence in proceedings, either a hearing by the local authority or a criminal trial. A master copy is retained for a period of one year in case the working copy becomes damaged or corrupted. The master copies are kept on a hard drive that is kept in a locked safe that is restricted to licensing staff only.

There is no encryption on the hard drive, but this is locked in a safe that is bolted to the ground and kept within the licensing office. Licensing do not share the office with any other department.

How will the data be deleted? E.g. Manually, via automated process etc.

Vehicle hard drives overwrite when storage is full, capacities are set so average time on the disc is 31 days.

Any downloaded data is then only kept in line with retention schedules which are dependent on the use of the download.

Data on the master copy hard drive is wiped annually and only data less than one year old is retained.

What is the source of the data? i.e. What is the flow of data into the Council?

Cameras/microphones in the vehicles, directly from data subjects.

Will you be sharing data with anyone?

INFO: If yes, please provide details

As per the Taxi camera Policy, data will only ever be shared on four occasions:

(i) where a crime report has been made involving the specific vehicle and the Police have formally requested that data or,

(ii) when the authority is notified in writing of a complaint in relation to a specific vehicle or driver and the matter cannot be resolved in any other way.

(iii) where a Data request is received from an applicant e.g. 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 or passenger.

(iv) Subject Access Request compliant with the General Data Protection Regulation.

If so, how will the data be transferred?

Once it has been established it is appropriate to conduct a download arrangements are made for a licensing officer to access the data box in the vehicle.

This is usually by contacting the proprietor and arranging for the vehicle to be brought to the licensing office, occasionally because of circumstances a vehicle is in police possession in a secure compound and staff visit the compound and are provided access by the police to facilitate the download.

There are two styles of data box, one where the box is secreted within the vehicle behind panels but with a lead accessible to staff to plug the download laptop into or the data box is in a locked position out of clear view, usually under a seat or in the boot.

Licensing staff have a key for the lock to remove the data box and perform the download in the office away from the car and driver. Once the data is downloaded onto the lap top computer the data box is refitted if it had been removed. A copy of the data is either burnt onto a data disc for the requestor and stored securely in the office awaiting collection or is securely uploaded to the requester's servers. Additionally, a copy of the data is transferred onto a separate hard drive that is kept in a locked safe within licensing. This is purged of data annually. The laptop copy is then deleted.

If the data is being shared, will this be governed by an agreement? e.g. contract, data sharing agreement, data processing agreement

Requests for data come in on an ad hoc basis. The police use their DP2 form which identifies the legal basis for the request and brief circumstances to justify such a request. Other agencies use the same process but in a different format of letter/communication.

Describe the scope of the processing

How often will the data be collected and used?

Data will only ever be decrypted, downloaded and used or shared in four circumstances, as set out in the policy referred to above:

(i) where a crime report has been made involving the specific vehicle and the Police have formally requested that data or,

(ii) when a substantive complaint has been made to the Council regarding a specific vehicle / driver and that complaint is evidenced in writing (and cannot be resolved in any other way),

(iii) where a Data request is received from an applicant e.g. 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.

(iv) Subject Access Request compliant with Data Protection legislation.

The following tables shows the number of camera downloads conducted in each year.

2019	71
2020	47
2021	82
2022	58
2023	69

How long will you keep the data, and how is this length of time justified?

The hard drives in the vehicles overwrite when the memory is full. The memory size is set so with average use of a vehicle approximately 31 days recording is captured before being over written.

Any downloaded data is then kept for as long as is necessary for the purpose it was secured and is retained in line with the retention schedule appropriate to the purpose and no longer than is necessary. Generally, cases involving prosecution are kept for 10 years, otherwise data is kept for a period of three years.

Data will only ever be downloaded in accordance with the taxi camera policy and the corresponding retention period is set out below:

(i) With the Police, where a crime report has been made involving the specific vehicle and they have formally requested that data – **the master copy will be held for 1 year**

(ii) By a third party or internal Council department (e.g. police or social services) where a Data request is received from them and they have a legitimate requirement to have access to the data requested to assist them in an investigation that involves a licensed vehicle or driver – **10 years, if the case involves prosecution, otherwise 3 years**

(iii) To a data subject after receiving a subject access request. – **6 years**

Is the time period reflected in the Council's Retention Schedule?
https://staffinfo.southampton.gov.uk/information-governance/records-management/retention.aspx

INFO: Please specify the corresponding entry on the Council's Retention Schedule. If unsure, contact the Information Officer (Data Management): records.management@southampton.gov.uk

The corresponding retention entry is set out below:

With the Police, where a crime report has been made involving the specific vehicle and they have formally requested that data – **BD9e**

(i) By a third party or internal Council department (e.g. police or social services) where a Data request is received from them and they have a

legitimate requirement to have access to the data requested to assist them in an investigation that involves a licensed vehicle or driver – **BD 9**

(ii) To a data subject after receiving a subject access request. – **A 4.27**

How many individuals are affected?

All occupants of licensed vehicles. Currently we license 283 hackney carriages and approximately 1150 private hire vehicles.

Some vehicles, predominantly chauffeur and limousine contract vehicles that are deemed low risk are exempted from the requirement to have a camera fitted.

This means just over 1400 vehicles currently have a camera fitted.

The exemption in respect of chauffeur and limousine contract vehicles is not pre-determined, and has to be applied for, justified, and generally only applies to high end luxury vehicles undertaking contract work.

This is defined as not standard private hire work, but work with known clients on a contract for a number of journeys, and not just one, or one and a return journey. Airport runs for non-business purposes are not considered to be within this definition.

The exemption was sought when the taxi cameras were first introduced. A number of the licence holders were conveying senior officials and businessmen, some linked to defence contracts. The clients had advised they would not use vehicles with cameras quoting security reasons for their objection.

The risks associated with this specific type of work is significantly less than standard private hire, the individuals are not vulnerable, they are well known to the licence holders and will have built up a trusted relationship. Southampton City Council has not received a complaint or investigated an incident in one of these vehicles where taxi camera evidence would have assisted.

What geographical area does it cover?

The cameras are designed to record the inside of licensed vehicles. Generally, vehicles licensed by Southampton operate within the city boundary or neighboring authorities, however there are a number of journeys that go much further.

The vehicles can operate anywhere within the UK. It should be noted Southampton City Council remain the licensing authority responsible for enforcement in relation to the vehicle and driver irrespective of their location (in relation to fitness and propriety).

Describe the context of the processing
What is the nature of your relationship with the individuals?
INFO: Detail who the data subjects will be (e.g. residents, carers, pupils, staff, professionals)
We are the licensing authority for the vehicle and driver being used. Data subjects will be drivers of licensed vehicles and their passengers (whether fare paying or not).
How much control will they have over their data? Will they be able to change it, access it, delete it etc.?
Individuals will not have direct access to the data, and can only view or receive a copy if the Council is satisfied there is a legal basis for them to have access e.g. through a Subject Access Request. Data subjects will also be able to exercise their right to object to the processing of their personal data. Service Area privacy notice updated with pathway to object. Any objection would result in a consideration of maintaining the policy and a decision by the authority on appropriate steps to take on a case-by-case basis. With regard to drivers, before any vehicle is licensed checks are conducted to ensure they meet the policy and conditions. Applicants are informed of the requirement to have an approved camera system fitted when they first get a driving licence and again when they apply for a vehicle licence. This is the likely trigger for any objections. This already occurs with executive vehicles used solely for contract hire, they seek an exemption at the application stage prior to the grant of a licence. The applicant is required to clearly set out their proposal on how they will operate the vehicle and any other reason for requesting an exemption. This is then considered through the application process. We would apply the policy we already have regards executive hire. Any objections received outside of that policy would be considered on a case-by-case basis, applying appropriate legislation as applicable to the case. An example was a Rolls Royce previously used by an international star that would only be used for novelty hire or in the production of films. The vehicle was clearly never going to be used for traditional private hire work and the risk associated with its use was low, an exemption was applied. Applicants for private hire vehicle licences have always had the option of licensing with other authorities as there are now a number of Operators that work using mobile phone apps which can allow drivers to licence in one authority area but work in another. When we introduced engine emission standards we saw a number of vehicles licence elsewhere, similarly when our knowledge test was more difficult than neighbouring authorities. We have never seen a loss of numbers linked to the camera policy.

Would they reasonably expect the Council to use their data in this way?
INFO: Please provide details to support your answer
Yes. The data is kept secure and only used when necessary in accordance with the policy. The vehicles are required to display appropriate notices/signs advising of the cameras. Regular checks are made to ensure these are in place. A copy of the sticker used is below.      Vehicles are only licensed for a year resulting in them attending the office at least annually when the vehicles are inspected and a check is made to ensure the correct sticker is in place. This is in addition to any other ad hoc inspection undertaken by council licensing staff. The signs direct individuals to the Council's online privacy policy, which contains specific information relating to the personal data captured by the cameras. The licensing webpage of the council advises of the requirement to fit cameras and have copies of the taxpolicy that details when downloads can be condicted. This provides protection to both the public and drivers. The drivers are in a position of power having control of the vehicle and where it goes so the public expect protection from an abuse of this position of power. Drivers are also vulnerable as they are on their own so open to attack and false and malicious accusations. In each case the cameras provide protection and the data used, when appropriate, to support any investigation linked to a licensed vehicle. Unlike a normal private vehicle a licensed vehicle is able to travel at any time in almost any location without raising suspicion, this makes them ideal vehicles to convey contraband or for other unlawful purposes.

Do they include children or other vulnerable groups?
INFO: If yes, please provide details
Yes. A lot of drivers rely on school contract work so take children, sometimes these children are unescorted. The situation is similar with Social Services contracts with vulnerable adults but to a lesser extent. The majority of taxi journeys do not involve children or vulnerable adults but most drivers will at some point take a child or vulnerable adult. Taxis are used more by the vulnerable in society proportionally compared to those that are not vulnerable. A large proportion of journeys at night are with people vulnerable through intoxication and the degree of vulnerability is extreme from slightly to unconscious. We acknowledge this may affect their ability to understand the cameras are in operation but we have addressed this with clear and simple signage.
Are you aware of any prior concerns over this type of processing or security flaws?
INFO: If yes, please provide details
We are aware of the concerns raised by the Information Commissioner's Office regarding the recording of non-fare paying journeys, however the practical experience of SCC is this concern has not been raised by taxi drivers or passengers with the exception of one incident where the issue was touched upon but not pursued. In this case a driver was investigated for a public order offence where he was accused of threatening and abusing a juvenile who he believed had been bullying his son, the footage also showed him driving whilst using his mobile phone, he was given a written warning about his driving as a result of what was seen on the download. The driver was accepting of this but a taxi owner questioned the use. There is general support for the scheme as it currently operates. Public surveys demonstrate support for the scheme. When the permanent recording of audio was stopped a large number of drivers expressed their objection to the removal of this as it provided them with protection, especially from abuse and racial abuse. The main complaint from the trade is the cost of the systems that is high because of the high level of encryption required.
Is the processing novel in any way? E.g. do other local authorities have a similar process in place?
INFO: If yes, please provide details
The Council are aware of 11 other local authorities that mandate cameras in their vehicles, but the Council is only aware of one other authority that requires the cameras to be operational whenever the vehicle is in use. The Council are also of the opinion a large number of authorities would like to have a similar scheme.

It believes that a significant number of authorities are waiting for better clarity from the Information Commissioner's Office on the position of data controller and the provision of an off switch as most consider the provision of an off switch significantly undermines the purpose of the cameras.

Licensing authorities are also concerned that mandating taxi cameras may encourage licence holders to licence elsewhere.

Are there any current issues of public concern that should be considered?

INFO: If yes, please provide details

Right to privacy when the vehicle is not being used as a licensed vehicle. However the vehicle remains a licensed vehicle regardless of the use it is being put to.

This is a principle that is well-established in licensing law and cases considering the point have determined that a licensed vehicle can never be driven by anyone other than a licensed driver (i.e. it not being used for hire does not make it a private vehicle at that time).

Criminal offences are committed if the vehicle is driven by an unlicensed driver. Case law has established that it is the nature of the vehicle, not the use to which it is put at any given time that determines its status. It is, therefore, a widely accepted position in licensing law that once a vehicle is licensed, it remains a licensed vehicle.

For these reasons, matters of policy and conditions attached to the vehicle licence must be complied with at all times – not simply when the vehicle is available for hire or is actually being hired.

That is because the vehicle, once licensed, could be put to those uses at any given time.

The vehicles are predominantly working in order to recover the costs and provide earnings. The actions of a driver are equally important whether in private or as a licensed driver.

No technology exists that can differentiate between a vehicle being used for a licensed purpose and a non-licensed purpose

The vehicle is required to obey all of the conditions whilst licensed, so it must display the plate and signage as required by our conditions.

These conditions make it extremely obvious to anyone it is a licensed vehicle, these displays cannot be turned on or off or removed easily (or lawfully) so the appearance of the vehicle will remain that of a licensed vehicle and anyone approaching the vehicle will have little doubt it is a licensed vehicle.

Since the cameras have been installed we continue to receive complaints of wrong doing by drivers that without camera evidence would be difficult to determine one way or the other. Previous examples are:-

.

1. Camera evidence corroborated numerous complaints of drivers texting whilst driving.
2. Taxi camera data confirms complaint that driver had his penis out whilst waiting for his passenger.

3. Taxi camera footage supports allegation driver sexually assaulted a single vulnerable female.
4. Driver with excess of 20 years driving with no complaint history conveys a vulnerable passenger and gets her to touch him intimately. The victim also alleges he had sex with her later that evening after he had finished work. The driver denied the allegation. The taxi camera data confirmed he did place her hand on his groin and corroborated the timings of him finishing work, exiting the vehicle and then returning at the times given by the victim.
5. Taxi camera data supported passenger account of careless driving by licensed driver
6. Taxi camera data support allegation driver was drinking alcohol whilst driving.
7. Taxi camera footage shows assault on a driver whilst waiting at a rank.
8. Taxi camera footage support allegation driver was using mobile phone whilst driving
9. Taxi camera data provided key evidence resulting in conviction of assault by penetration resulting in substantial prison sentence. Driver was in licensed private hire vehicle, the audio activation button had a fault resulting in audio permanently recording. Driver heard attracting lone vulnerable female late at night into car by saying she was safe he was a licensed driver. He took her without a booking so 'off duty' and went to an isolated car park where he engaged in sexual activity with her for over 2 hours. Audio data was key in determining whether valid consent had been given. Without the taxi camera evidence the police would not have been able to secure a conviction.
10. Taxi camera data used to support allegation of inappropriate behaviour towards a lone female by obtaining her phone number before allowing her out of the car.
11. Taxi camera shows driver using mobile device whilst driving with fare paying passenger on board
12. Taxi camera footage confirming allegation driver was exposing himself in a public area.

This demonstrates drivers will pose a threat to vulnerable members of the public, commit crimes and some take direct steps to prevent the camera recording the data. The provision of an off switch, whether it has a delay or not will not counter this behavior. Example 9 provides evidence why an off switch should not be introduced and supports the call to permanently record audio as well.

As inappropriate behaviour, in particular, towards women is now being reported and acted upon we are seeing a significant increase in reports of drivers having inappropriate conversations or making inappropriate comments to lone vulnerable women. Evidence indicates the majority of these incidents occur at night. Currently we have to rely upon a corroborating incident or evidence in order for us to take firm action against a driver. Drivers are vulnerable to false allegations however passengers are at risk from drivers. We have revoked driver licences when we have the corroborating evidence. Permanent recording of audio is an option to address this risk, whether permanently or during specific hours.

Describe the purposes of the processing
What do you want to achieve?
Public confidence in the use of licensed vehicles and drivers feeling protected and safe when driving a licensed vehicle. The promotion of public safety (including the safety of drivers).
What is the intended effect on individuals?
Greater safety and protection from harm when travelling in or driving a licensed vehicle. A sense of feeling secure and safe.
What are the benefits of the processing – for the Council, and more broadly?
INFO: Please confirm which of the Council's key outcomes this will support, and how
Outcome: ☐ Southampton has strong and sustainable economic growth ☐ Children and young people get a good start in life ☒ People in Southampton live safe, healthy, independent lives ☐ Southampton is an attractive modern city, where people are proud to live and work
Please explain how the outcome is met
The Council upholds it obligations under the Local Government (Miscellaneous Provisions) Act 1976 (ensuring drivers of vehicles are fit and proper and promoting public safety through attaching conditions and adopting appropriate policies) and Section 7 Crime and disorder Act. Public confidence in the hackney and private hire industry is maintained. Reduction in incidents of inappropriate behavior and crime by both drivers and public.

Step 3: Consultation

Consider how to consult with relevant stakeholders
Do you think it's necessary to consult with the public about the processing? If not, why?
INFO: Please provide details to support your answer
Yes. This is recording of sensitive data in the public domain. The public need to understand the purpose of the scheme and to express their opinions whether

supportive or not and these need to be continually considered as the policy is reviewed.

The taxi policy is to be reviewed every 5 years and this will include a public consultation. The hackney carriage unmet demand survey is conducted every three years and we normally include questions in this on the taxi camera. Quarterly meetings are held with taxi trade representatives.

In the unmet demand survey conducted in 2022 we asked:-

Southampton City Council has a policy of fitting video cameras in licensed vehicles to permanently record video and, upon activation of a panic button, to record audio. The purpose is to improve safety. Do you feel safer travelling in a Southampton licensed vehicle knowing that all vehicles are fitted with a camera system?

The responses were:-

Yes 82%

No 18%

The video cameras in licensed vehicles currently operate all the time the vehicle is in operation, whether or not it has been hired. If drivers were given an off switch for their camera system to address privacy concerns when the driver is using the licensed vehicle for their private use (for example, with members of their own family), would you feel less safe using Southampton licensed taxis?

The responses were:-

Yes 54%

No 46%

Who else do you need to involve, or have you already involved within the Council?

INFO: e.g. IT services, records management

We liaise closely with the Data Protection team, however, on a day-to-day basis they only see the SAR details. No other team or department are involved and only approved officers within the team have access to the data. We liaise with legal, the Data Protection team and IT with the implementation of policy and its review.

Do you plan to consult IT, external information security experts, or any other experts? If not, why?
INFO: Please provide details to support your answer
IT services will be consulted with regards any ongoing security concerns. We keep in regular contact with the suppliers who understand the need for secure systems.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures
What do you consider your lawful basis for processing to be? Please choose one of the following…
INFO: There should generally only be one legal basis for processing.
☐ The data subject has given consent ☐ The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☐ The processing is necessary for compliance with a legal obligation to which the Council is subject ☒ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council ☐ The processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party
Please provide further information to support this
INFO: For example, if the processing is necessary in order for the Council to perform a statutory function, detail the relevant legislation.
The Council relies on these various processing conditions, on the footing that the processing is necessary to enable the Council to discharge its functions under a wide range of legislation. These include the following: • Functions in relation to licensing taxis and PHVs: see the Local Government (Miscellaneous Provisions) Act 1976 and 1982, and the Town Police Clauses Act 1847 and 1875. • Requirements to have regard to safety, crime and disorder. See section 17 of the Crime and Disorder Act 2017: duty of local authority to exercise its functions with due regard to the need to prevent crime, disorder and anti-social behaviour.

Why is the processing deemed necessary?

INFO: e.g. Is the Council under an obligation to provide a service, or is there a particular problem that the project is trying to address?

The taxi profession has been identified as a position of trust and responsibility within the community that could be abused and as such is listed as an exception to the Rehabilitation of offenders Act 1974.

There are historical and continuing cases of taxi drivers abusing their position of trust and of taxi drivers being assaulted and abused by members of the public. Often these cases have no independent evidence to support either the accuser of the accused. A high proportion of taxi users are vulnerable at the time of use and the drivers are alone with passengers in remote areas making them vulnerable to attack. The taxi cameras provide independent reliable evidence of events and we have anecdotal evidence of it preventing crimes and improving behaviors.

SCC does have a more active Night-Time Economy than neighbouring authorities, and it is generally at night when members of the public and taxi-drivers are more at risk from violence, crime, abuse, and anti-social behaviour.

Does the processing actually achieve your purpose?

INFO: Please provide details to support your answer

It is not possible to compare data now with before the introduction of the camera policy in 2009. However, it is clear the cameras are extremely useful in providing independent corroborating evidence when such allegations are made. This protects both the drivers and the public. It also empowers the authorities to take appropriate action.

There continues to be allegations of sexual assault, kissing and groping, this is mainly when the victims are intoxicated. Please see examples above. The incident of the driver with a 20-year unblemished record have sexual contact with a vulnerable victim in the car followed by him visiting her after work and having sex with her clearly demonstrates the benefit and need of no off switch. Further the example of a driver using the fact he was in a licensed vehicle and a licensed driver to entice a lone, vulnerable female who was not a fee paying customer, into his vehicle before subjecting her to over 2 hours of sexual activity demonstrates the need for licensed vehicles to have cameras and with audio recordings.

There have been very few serious assaults reported by drivers since the cameras were introduced. We receive anecdotal evidence of better behavior by passengers when they notice the cameras.

When permanent audio recording was stopped, we had numerous drivers complaining, asking for the audio to remain as it protected them from racial abuse. The lack of audio recording is hampering investigations of inappropriate conversations where individuals are made to feel vulnerable and behaviour tantamount to grooming is described.

A survey asked if people agreed to the taxi camera policy, at the ranks the response was 67% agreed, on line 97% agreed. Security cameras was one of the reasons given by the public that made them feel safe using taxis.

Is there another way to achieve the same outcome?
INFO: Please details to support your answer
The Council considers that a requirement to have permanently recording data is the only way to keep the public safe. The vehicle remains licensed all of the time, regardless of the use it is put to at the time. The behavior of the driver remains important in the assessment of being a fit and proper person all of the time, not just when acting as a licensed driver. Any person entering the vehicle will see the signs and expect the protection the cameras provide. The drivers have a right to privacy but must acknowledge a lower expectation when driving a licensed vehicle. As it is not possible to actively monitor the footage, it is not possible to determine when a driver is undertaking a private journey or a working journey. There is no protocol or system that can currently differentiate the type of use the vehicle is being put to, however the driver and vehicle remain licensed at all the times the licence is in effect. The alternative is to have a system for visual recording where the driver can choose whether or not to trigger recording; for the reasons set out below, the Council does not consider that this is a satisfactory approach. The Council is aware that other licensing authorities adopt such systems, whereby the driver can manually turn off the cameras (e.g. the visual recording equipment automatically comes into operation when the ignition is turned on. In order to stop it, the driver needs to leave the ignition running, leave the vehicle, open the boot, and switch off the equipment using the switch in the boot). This creates a risk that the Council are unwilling to accept, that can be illustrated by the following examples: 1. A driver is transporting a fee-paying passenger. They make an excuse to leave the vehicle briefly (e.g. they say that they needs to check if they have a puncture), leaving the engine running while they do so. They turn off the recording equipment using the switch in the boot of the vehicle, and then get back into the vehicle. They can now assault the passenger without anything being recorded. If the passenger subsequently complains, and there is no recording, the driver can say that the passenger got out at the point where they left the vehicle, and that they then turned off the recording equipment at that point as they no longer had a passenger. There will be no way of verifying whether the driver is telling the truth. 2. A driver switches off the recording equipment after dropping off a fee-paying passenger. They continue driving, and pick up fee-paying passengers, without turning the equipment on. There would be no record available to the Council as to whether or not the driver was transporting fee-paying passengers while the engine was switched off. 3. A driver switches off the recording equipment and then provides individuals with lifts, for free. This is private use: i.e. the sort of use that could potentially give rise to an expectation of privacy. However, there is an elevated risk to passengers, and it is the livery and get-up of a licensed vehicle that creates this risk. Passengers are

more likely to trust a licensed vehicle (even when it is not operating for hire), than to trust an offer of a lift from a stranger in an ordinary unmarked vehicle.

4. A driver switches off the recording equipment and then uses the vehicle for an unlawful purpose not involving the transport of passengers (e.g. they use it to transport drugs). There is an elevated risk of this kind of use (as compared with the risks presented by an ordinary vehicle), because a vehicle that is visibly a licensed vehicle is less likely to be stopped or challenged (e.g. by the police).

The following alternatives have also been considered, and rejected for the reasons given below:

A policy of continuous visual recording which does not need to be operational when the vehicle is not being used for licensed purposes

Any such policy could only work if the driver was able to disable the recording system, and this would create a risk that the driver would do so while transporting a paying passenger.

Combining a less intrusive use of visual recording with a parallel automated system (which could be audited) to record when a driver clocks on and off duty

A driver who had “clocked off” under this system could not be prevented from carrying paying passengers after clocking off.

A system to alert a driver during on-duty hours that the system is not operational

This suggestion addresses the risk of accidental deactivation of the system when paying passengers are on board. It does not address the risk of deliberate deactivation.

Electronic recording of when the system is deactivated and reactivated, for consistency checks

The difficulty is that if the driver asserted that they had not carried paying passengers while the system was deactivated, then there would be no way for the Council to verify this.

A recording system based on times of day when the driver would be on shift, and/or the use of panic buttons

This suggestion seems to assume that if the visual system was not in operation then the passenger could use a panic button in order to trigger it. There are a number of difficulties here. The passenger would need to be able to locate the panic button, and would need the presence of mind to use it.

This would be challenging if the passenger was being subjected to physical or sexual assault, and/or concerned not to escalate a confrontational situation between themselves and the driver.

The use of a panic button would be particularly problematic for vulnerable passengers: e.g. children, the elderly, those with physical or mental impairments, or those temporarily affected by drink or drugs. These are precisely the categories that the Council is especially concerned to protect.

A more intensive use of existing licensing and control powers, including vetting

This does not meet the concern that an ill-intentioned driver might deliberately turn off visual recording, even with a paid passenger on board, and then lie in order to cover their tracks if challenged.

Implementing a "cover system" to allow drivers to cover the camera with a sign (that would alert passengers that the camera is not in use), when the vehicle is being used for personal business

Due to the nature of the camera design, there would be practical issues in implementing this system, and it would also not be possible to confirm that the approved cover was being used by the driver. It would also require the driver to remove the cover when the vehicle was being used for licensed activities, and would be easily open to abuse.

Suspending the vehicle licence and turning off the cameras when the vehicle is to be used for personal business

Whilst this approach is currently taken where a vehicle is to be used for long, uninterrupted periods of personal use (e.g. a driver taking the vehicle on holiday), it would not be a practical approach if drivers wished to have the cameras turned off when "off shift". Suspending and reinstating a licence is not a simple process, and turning the cameras on and off on this scale would require an increase in staff and resources, this in turn will lead to an increase in fees to recover the additional costs.

As stated above, the Council continues to engage with key stakeholders about the camera policy. There are two surveys due to take place; the unmet demand survey , which will aim to seek views from the public and drivers on the current system in place, and its operation, and a survey specifically for private hire drivers, which is due to take places over the next few months. The Council will use these surveys to seek views on alternative methods of operation, both from the trade and the members of public.

The Council continues to keep the matter under review, and will continue to consider: (a) evidence about any other technical solutions besides those identified so far; (b) evidence about the use that is made of information that is collected under the existing policy; and (c) evidence about the public's view of its current policies.

There is limited flexibility, however, due to the nature of the law around taxis; a vehicle, once licensed, never ceases to be a licensed vehicle during the currency of the licence. Furthermore, a licensed vehicle can never be driven by anyone other than a licensed driver.

How will you prevent function creep?
INFO: Function creep is where data collected for one purpose is used for another purpose over time.
The acceptable use of the cameras is detailed in the Council's Taxi Policy. This is reviewed regularly. The last change to the policy was in August 2022. The licensing authority has no desire to 'monitor' the behavior of drivers through the use of cameras. It is only when there is good cause to review data that we will wish to view the data. In a similar vein we have no desire to fit trackers to the vehicles to see where they have been.
How will you ensure data quality and data minimisation?
INFO: We should only use the minimum amount of personal data possible to achieve the purpose of the processing.
See generally the taxi policy, in relation to the use made of data. Audio is only activated for 5 minutes via a button accessible to the driver, Cameras are specifically designed to operate inside the cabin of the vehicle, providing sufficient quality to identify suspects and activity within the cab but quality diminishes for activity outside of the vehicle. Cameras are positioned high on the front windscreen and look down towards the occupants. The recording systems have to meet the specification set by SCC. SCC were aware that some early model systems reported failures, but these are not present on the newer models, which have replaced these. Whilst a fault may not be apparent in all cases until a download is required, vehicles are subject to inspections at least annually. If a vehicle's camera system is found to have a fault, that vehicle licence will be suspended until the fault has been fixed.
What information will you give individuals about the processing?
Any applicant for a vehicle licence will be advised of the requirement to have a camera fitted. New drivers are personally briefed on the cameras, The Council is in the process of including the use of cameras in the safeguarding training that all drivers have to undertake and refresh every 3 years. Various pages on the Council website on taxi licensing make reference to the taxi cameras, and the continuous recording. The cameras are overtly fitted in the vehicle and all the cars are regularly checked to ensure appropriate signage The policy is available on the council website.

Aside from existing corporate processes, will there be any additional measures in place to support individuals exercising their privacy rights?
INFO: Data subject's rights include the right to access, rectify, erase, port, and restrict their data. Additional measures could include self-service options to enable individuals to change / update their personal data, or download copies of their data
Policies are published on the Council website, which is linked to via the signage in the vehicle., Staff are aware of the processes and advise enquirers. Drivers are made aware of the cameras and camera policy during the licensing process. Conditions attached to vehicle licences make the requirement clear. Save for the operation of the Taxi policy subject access requests and the data collected is subject to wider SCC policies on data protection.
If a third party is carrying out the processing on our behalf, what measures will be in place to ensure they comply with the UK GDPR, and assist the Council in supporting individuals in exercising their rights?
INFO: E.g. will there be a contract in place with the third party that contains data protection obligations?
The proprietors and drivers are considered to be processors, as they own the equipment that is used to capture, recorded, and store the Council's personal data. The licence application forms will need to identify this and explain their responsibilities. The Councilenters into a Data Processing agreement with all proprietors when they apply for a new vehicle licence. Driver training is provided by the installer to the driver at that point, and when a driver is issued with a new driver licence, they are given training by an enforcement officer on appropriate use of the camera system. Also safeguarding training undertaken every three years by drivers includes camera usage
How do you safeguard any international transfers of personal data?
INFO: If there are no international transfers involved, please state this
There are no international transfers of data.

Step 5: Send DPIA Form to the Data Protection Officer

After completing this part of the form, please send the document to the Information Lawyer (Data Protection Officer) at dataprotection@southampton.gov.uk
The DPO will review the information provided, and identify and assess the privacy risks.

Step 6: Identify and assess risks (DPO to complete)

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. As the CCTV systems are activated whenever the vehicle is running, they operate continuously, including when the taxi is being used privately by the driver. Where a taxi is being used by a driver for their own private or domestic purpose, there is a risk that continuous recording will capture information that is irrelevant and unnecessary for its purpose. Whilst it is probable that private data will be captured by the cameras, the severity of harm caused by this is minimal for the following reasons: • The footage is stored in the vehicle in encrypted form • The Council has a system that includes an exceptional level of security, and only staff within the Licensing team can download the footage; is not accessible to the driver or anyone else. • Downloads can only take place under limited circumstances, and must adhere to the Council's Taxi policy • A vehicle, once licensed, never ceases to be a licensed (and therefore commercial) vehicle during the currency of the licence, and a licensed vehicle can never be driven by anyone other than a licensed driver. It is the Council's view, therefore, that licensed drivers have a lower expectation of privacy when driving licensed vehicles, and will be aware of their ongoing duty as to behaviour and professional standards whilst doing so. • A licensing authority has a legitimate interest in how a licensed vehicle is being used and how the driver is behaving at all times, whether or not the vehicle is being used to transport fee-paying passengers. Given the extensive controls over access to and use of the visual images recorded in licensed vehicles, it cannot be said that the	Probable	Minimal	Medium

approach taken by the Council reduces drivers' or passengers' private social life to zero. Moreover, even assuming that Article 8 of the Human Rights Act 1998 is engaged, the level of intrusion is very limited and is justified by the considerations set out in the DPIA.			
2. There are concerns regarding the adequacy of the security measures in place to protect the personal data captured by the systems, in particular the hard drive on which the videos are stored; whilst this is stored in a safe within a locked room, the drive itself is not encrypted. If a motivated intruder were able to access this drive, they would have access to video (and potentially audio) information relating to drivers (acting in a professional capacity), and their passengers. The footage may contain information relating to criminal offences, due to the reasons why it may have been deemed necessary to retain a copy of the footage.	Remote	Minimal	Low
3. Whilst there are clear retention periods set out in the Council's retention schedule for copies of the footage used for investigations, prosecutions, and subject access requests, retention relating to third party requests is not detailed. This may lead to the data being held for longer than is necessary, also increasing the security risks associated with this data.	Remote	Minimal	Low
4. Whilst this is addressed in the Council's privacy notice, which is linked to via the stickers in the vehicles, the specific process to enable data subjects to exercise their right to object to the processing is unclear. As such, data subjects may not be aware that they have that right in relation to this processing, or the steps they need to take to exercise this right. Individuals must be able to exercise both their right to object to the process, and their right to restrict that processing whilst an objection is being considered, especially where they feel that their interests, rights, and freedoms are being overridden by the processing.	Remote	Minimal	Low

5. Whilst fair processing notices are placed inside vehicles, and inspected regularly, it is not clear what requirements are imposed on the drivers / proprietors in relation to these stickers, and how those requirements are enforced. As such, there is a risk that drivers and passengers will not have received fair notice in respect of the processing, or be provided with important information about the processing.	Remote	Minimal	Low
6. Whilst the relationship between the Council and the vehicle owners (and to an extent, the drivers), is that of data controller / data processor, it is unclear as to what measures are in place to govern that relationship, or what training is in place around the use of the cameras. This lack of governance could lead to increased security risks, lack of assurance, and barriers to data subjects being able to exercise their privacy rights.	Remote	Minimal	Low
7. Although surveys were undertaken to ascertain driver and passenger opinion on the cameras and their usage, subsequent surveys were either delayed or postponed due to the Covid-19 pandemic. Not having up-to-date opinions on the processing hinders an informed decision about its necessity, proportionality, and adequacy being made.	Remote	Minimal	Low

Step 7: Identify legal basis and measures to reduce risk (DPO to complete)

Condition(s) for Processing
Personal Data
☐ The data subject has given consent ☐ The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☐ The processing is necessary for compliance with a legal obligation to which the Council is subject ☒ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council ☐ The processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party
Further Information
The Council relies on these various processing conditions, on the footing that the processing is necessary to enable the Council to discharge its functions under a wide range of legislation. These include the following: Functions in relation to licensing taxis and PHVs: see the Local Government (Miscellaneous Provisions) Act 1976 and 1982, and the Town Police Clauses Act 1847 and 1875. Requirements to have regard to safety, crime and disorder. See section 17 of the Crime and Disorder Act 2017: duty of local authority to exercise its functions with due regard to the need to prevent crime, disorder and anti-social behaviour. The Council recognises that the question of whether processing is necessary for the purpose of the various conditions relied upon involves an assessment as to proportionality, comparable to the assessment that would arise in the context of a qualified right under the ECHR: see South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55. By reason of the matters set out above, as to the justification for operation of the system, the Council considers that this requirement is satisfied. When making the proportionality assessment it is essential to consider, not only the benefits secured by system, but also the extent of its impact on individuals. In reality, the impact is very modest indeed: the images that are recorded are kept secure, cannot be viewed by the driver, are decrypted and downloaded only if needed, and otherwise are automatically overwritten within a short period of time. By contrast, the system delivers real and substantial benefits for the protection of both drivers and passengers.

Special Categories of Personal Data
☐ The data subject has given explicit consent ☐ The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law ☒ The processing is necessary for reasons of substantial public interest ☐ The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems ☐ The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ☐ No special category data being processed
Further Information
The Council contends that the processing is in the substantial public interest, given the importance of the objectives pursued by the system, and given that a less intrusive system would not meet those objectives. In accordance with Department for Transport issued Best Practice Guidance, the aim of local authority licensing of the taxi and PHV trades is to protect the public. As such, public protection must be at the forefront of decisions regarding the discharge of the Council's licensing functions. The licensing process places a duty on the local authority to protect the public. Given the nature of the role, it is paramount that those seeking a living in the trades meet the required standards, and there is public trust and confidence in the overall safety and integrity of the process. The use of the cameras provides the public with that trust and confidence, as can be demonstrated by the most recent unmet demand survey responses referred to in this DPIA, where the vast majority of respondents agreed with the Council's taxi camera policy, citing security cameras as one of the reasons that made them feel safe using taxis.
Data Protection Act 2018 Schedule 1 Condition
Schedule 1, Part 2, Paragraph 6 - Statutory etc. and government purposes.

Further Information
As stated, the Council relies on these various processing conditions, on the footing that the processing is necessary to enable the Council to discharge its functions under a wide range of legislation. These include the following: • Functions in relation to licensing taxis and PHVs: see the Local Government (Miscellaneous Provisions) Act 1976 and 1982, and the Town Police Clauses Act 1847 and 1875. • Requirements to have regard to safety, crime and disorder. See section 17 of the Crime and Disorder Act 2017: duty of local authority to exercise its functions with due regard to the need to prevent crime, disorder and anti-social behaviour

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5			
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**
1.	It is not possible for the cameras to automatically distinguish private use from commercial use, and the only way to avoid continuous recording would be to give drivers the ability to manually turn the cameras on and off. The Council has considered this option and rejected it, for the following reasons. A vehicle, once licensed, never ceases to be a licensed vehicle during the currency of the licence. Furthermore, a licensed vehicle can never be driven by anyone other than a licensed driver. For these reasons, matters of policy and conditions attached to the vehicle licence must be complied with at all times – not simply when the vehicle is available for hire or is actually being hired. A mandatory system is not mandatory if it can be turned off at will, and this would defeat the purpose of the cameras, which is to protect both the passengers and drivers of the vehicles. The Council has a strong view that handing control of the system to the driver in this way will allow the most determined and dangerous drivers to abuse their position and will be most damaging for the safety of the most vulnerable passengers As such, this risk cannot be eliminated or reduced, and needs to be accepted by the IAO and SIRO.	Accepted	Medium

2.	The service area needs to review its current information security policies and procedures regarding the process. The Data Protection Officer should be notified of the outcome of the review, so that the DPIA can be updated, and a further assessment of the associated risks can be made. *[UPDATE 07/02/23] Service area have reviewed security measures, and are satisfied that they are appropriate (i.e. the likelihood of an individual breaching the security measures is low) [/UPDATE]*	If review does not lead to measures that eliminate or reduce the risk, this will have to be accepted	Low or Eliminated *[UPDATE 07/02/23] Low risk accepted [/UPDATE]*
3.	The service area must liaise with the Senior Records Officer to ensure that all retention periods relating to the processing are detailed in the Council's retention schedule. *[UPDATE 18/04/23] Retention schedule being updated. DPIA amended with entry information [/UPDATE]*	Eliminated	N/A
4.	The service area needs to review its current process in relation to the right to object to this processing, in particular confirming: • What steps are taken by the service area to inform individuals of their right to object? • What steps would the service area take if an individual made an objection? • Who would decide whether the objection should be upheld? The Data Protection Officer should be included in the review and the DPIA updated, so a further assessment of the associated risks can be made. *[UPDATE 07/02/23] Service Area privacy notice updated with pathway to object. Any objection would result in a consideration of maintaining the policy and a decision by the authority on appropriate steps to take on a case-by-case basis [/UPDATE]*	If review does not lead to measures that eliminate or reduce the risk, this will have to be accepted	Low or Eliminated *[UPDATE 07/02/23] Risk eliminated [/UPDATE]*
5.	The service area needs to review its current arrangements in relation fair notice stickers placed inside and outside of the vehicles, including • What requirements are imposed on drivers/proprietors in relation to these stickers • How those requirements are enforced • What steps are taken to ensure that the stickers are correctly placed The Data Protection Officer should be notified of the outcome of the review, so that the DPIA can be	If review does not lead to measures that eliminate or reduce the risk, this will have to	Low or Eliminated *[UPDATE 07/02/23] Risk Eliminated [/UPDATE]*

	updated, and a further assessment of the associated risks can be made. *[UPDATE 07/02/23] The service area has now mandated it for approved fair notice stickers to be displayed in vehicles [/UDPATE]*	be accepted	
6.	The service area needs to review its current governance arrangements regarding the processing relationship between the Council, as data controller, and the vehicle owners / drivers, as data processors. The review should include: • How compliance with Article 28 of the GDPR can be assured • A review of its existing relevant policy documents • Its current approach to driver training The Data Protection Officer should be included in the review and the DPIA updated, so a further assessment of the associated risks can be made. *[UPDATE 07/02/23] The Council now enters into a Data Processing agreement with all proprietors when they apply for a new vehicle licence. Driver training is provided by the installer to the driver at that point, and when a driver is issued with a new driver licence, they are given training by an enforcement officer on appropriate use of the camera system. Also safeguarding training undertaken every three years by drivers includes camera usage. [/UPDATE]*	If review does not lead to measures that eliminate or reduce the risk, this will have to be accepted	Low or Eliminated *[UPDATE 07/02/23] Risk Eliminated [/UPDATE]*
7.	The service area should ensure that the DPIA is updated with the most recent survey results in relation to the use of cameras, and ensure that opinions of drivers and the public are sought where possible in all future surveys. The DPIA should be kept updated with the most recent survey results. *[UPDATE 18/04/23] DPIA updated with the most recent survey results. [/UPDATE]*	Eliminated	N/A

Comments from the Data Protection Officer
Aside from those identified in section 6, the DPO is satisfied that all reasonable privacy risks have been identified and addressed. Whilst no high residual risks remain, SIRO sign-off is recommended, due to the high-profile nature of this project.

Comments from the Information Officer (Data Management)
No additional comments.
Comments from the Head of IT
Not consulted, due to the use of existing / established systems.

Step 8: Sign off

Item	Date	Notes
DPO reviewed DPIA and provided advice on:	14th October 2022	DPO should advise on compliance, step 7 measures and whether processing can proceed
Information Officer (Data Management) reviewed DPIA on:	17th October 2022	SRO should advise on records management matters
Head of IT reviewed DPIA on:	N/A	Head of IT should advise on IT security matters
Measures approved by Project Lead on:	27th October 2022	Integrate actions back into project plan, with date and responsibility for completion
Comments from Project Lead:	No comments.	
Residual risks approved by Information Asset Owner / Administrator on:	25th November 2022	The relevant IAO or IAA is required to accept any residual risks associated with the processing.
Comments from IAO / IAA:	No comments.	
Project approved by Caldicott Guardian (CG) on:	N/A	The relevant Caldicott Guardian is required to approve any project involving the processing of social care data.
Comments from CG:	N/A	
Residual high risks approved by the Senior Information Risk Owner (SIRO) on:	28th November 2022	If accepting any residual high risk, consult the ICO before going ahead
Comments from SIRO:	No comments.	

Step 9: Review

Item	Date	Comments
DPO reviewed DPIA on:	18/04/23	All actions completed
Date of next review:	18/07/23	
DPO reviewed DPIA on:	05/01/24	No new privacy risks introduced
Date of next review:	05/04/24	