Privacy Impact Assessment

Guidance and Template

1. Introduction to privacy

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

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

We are concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;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

2. Purpose

The purpose is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

3. Key Points

- A PIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.

- Conducting a PIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.

- The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

- Conducting a PIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

NB: the term project is used in a broad and flexible way – it means any plan or proposal…i.e.

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.

Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring

4. Identifying then need for a PIA

Answering yes to one of the following screening questions confirms the need for a PIA.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other
- information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

5. Overview of the Privacy Impact Assessment Process

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

WARRINGTON
Borough Council

Appendix 1: The Privacy Impact Assessment Template

Privacy Impact Assessment for:	CCTV within licenced taxis
Information Asset Register Reference:	IAR

Version	Date amended	Amended by	Changes
1.1	9/5/2016	Caroline Sharkey/Dave Watson	Amends into revised template
1.2	10/5/2016	Sarah Gallear	IG review of the document
1.3	03/10/2016	Andrew Robinson	Re-draft following ICO visit
1.4	04/10/2016	Sarah Gallear	Document amended following meeting with licencing colleaques & ERGE IGG rep

Identify the need for a PIA
Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

This PIA is for...	
A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV)	X
Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring	
The purpose is to... *select* as *appropriate*	
Promote use of and protect community facility and staff	
Provide assurance and protection to service users	X
Prevention and detection of crime	X

Purpose

The implementation of CCTV within licensed vehicles will serve multiple purposes which ultimately will enable the prevention and detection of crime and promote a safe experience for both drivers and the travelling public

The purposes include:-

- The protection of licensed drivers
- The protection of the travelling public
- The protection of contracted support

- To ensure that licensed drivers continue to be 'fit and proper' in line with the licensing conditions

The protection of licensed drivers

Information obtained from the Specialist Transport Services Manager shows that in the last 2 years they have terminated 8 taxi contracts as a consequence of hearsay evidence. CCTV footage would have allowed the hearing to consider the CCTV evidence and make a more informed assessment before reaching their decision.

Drivers work alone, often at antisocial hours, visiting areas that may be poorly lit or away from safe routes, and could be carrying any amount of cash within the taxi cab. These factors could increase the risk posed to the driver. Violent assaults in general have increased in the Town Centre after 12pm.

A significant proportion, estimated at 40% in 2015, of drivers are from an ethnic background. Data collected from Community Safety Partnership shows that hate crime incidents in Warrington for the year 2013/14 is recorded as 74 and in 2014/15 is recorded as 62.

Since the implementation of the CCTV in licensed vehicles in June we have been required to access CCTV footage to provide evidence for:-

- Racial abuse and physical assaults of drivers
- Passengers making off without payment
- Investigation on inappropriate behaviour
- Rape allegations
- Investigation on passenger stealing property found in taxi

The protection of taxi passengers

Licensed vehicles are used extensively to service the late night economy, the period of which extends well beyond the availability of other forms of public transport. Patrons often have little choice but to use licensed vehicles. Some customers may be vulnerable if they have consumed excessive amounts of alcohol, and or, become separated from their friends. Licensed vehicles are often the only option for vulnerable people who have no direct transport links, or who have special transportation requirements.

Without the benefit of CCTV an example of risks identified are evident in the following case studies:-

1. Police often have insufficient information to take a prosecution.
2. Victims do not receive appropriate restitution.
3. Drivers may continue to trade for extended periods; whilst any appeal is determined, potentially placing other vulnerable people at risk.
4. Lack of evidence to effectively deal with the first instance meant the driver was still able to trade, which resulted in a second unrelated allegation of a serious sexual assault (see below case study 1).
5. The availability of a more robust evidence base would have, in all likelihood,

secured a more timely resolution in both cases.

Case Studies

Study 1: Driver A was the subject of a serious allegation that they had acted inappropriately towards a lone female passenger. A, warning was issued and a record maintained on file due to insufficient evidence, Driver A continued to trade. Driver A was later arrested on suspicion of a further sexual assault in an unrelated incident. The Licence was suspended. Police had insufficient evidence to secure a prosecution and the suspension was lifted pending the licensing hearing. The Committee determined to revoke the licence. Driver A successfully appealed to the magistrate's court and was able to trade throughout the appeal process. The Licensing Authority appealed to the Crown Court and the decision to revoke the licence upheld.

Study 2: Driver B was reported to the Police following a serious allegation of sexual assault. Driver B was not paid for the fare and returned the same evening to take the person C to the cash machine. Person C did not withdraw any money but performed a sexual act on Driver B, whilst he was driving. Driver B stated that he did not instigate or consent to the act. The Licensing Committee determined to revoke the licence. Driver B appealed to both the magistrates and Crown Court, both appeals were dismissed.

The introduction of CCTV allows the Council with strategic partners to work with the trade, taxi marshals and street pastors to signpost people towards vehicles which operate to the highest standards of public safety. The availability of CCTV would increase the fear of sanction and reduce the likelihood of an incident occurring. In the event that a serious incident was to occur, or an allegation be made, then the availability of CCTV would enable an evidence based decision to be made, as to whether a crime has been committed, and increase the likelihood of securing an appropriate sanction.

The protection of contracted support

Case studies for incidents relating to transport provided by the Specialist Transport Unit before CCTV was installed

Specialist Transport cases where taxi drivers contracts have been terminated on hearsay evidence.

<u>Case Study 1</u>

Driver A was accused of physically abusing a child whilst on a school transport contract. This complaint was reported by the student's mother. Driver A was interviewed and denied hitting the child but confirmed that physical force was required to calm the child down. The contract was terminated. If CCTV was available in the vehicle it would have assisted in investigating the matter and clarifying the situation.

Case Study 2

Driver B was accused of putting a child he was transporting whilst on a school contract on the phone to one of his friends. Family and school reported it as a possible 'grooming' incident. Driver B was interviewed and denied that he had the child on the phone to his friend just that he had overheard the conversation. Driver B's contract with Specialist Transport was terminated. If CCTV was available in the vehicle it would have assisted in investigating the matter and clarifying the situation.

Case Study 3

Driver C was accused of slapping a child across the face whilst working on a school transport contract. The School reported it as a safeguarding issue to officers in WBC Specialist Transport Unit. Driver C was interviewed and denied the allegations. Driver C's contract was suspended with immediate effect. If CCTV was available in the vehicle it would have assisted in investigating the matter and clarifying the situation.

Since June 2016 we have been required to access CCTV footage to provide evidence for:-

- Service user assaulting an escort on a school transport journey provided by the Specialist Transport Unit

To ensure that licensed drivers remain to be 'fit and proper' persons to continue holding their joint Hackney/Private Hire drivers licence.

A driver's behaviour even when not on duty, particularly when in charge of a vehicle, can be taken into account when applications and renewals for a license are considered. A taxi is a licenced vehicle at all times and is marked as such with identification plates even when being used for personal journeys. Where the Council receives a complaint, it has to investigate whether the licensed driver remains compliant with the licensing conditions, including being a 'fit and proper person'.

It is established in case law that once a vehicle is licensed as a taxi or for private hire it remains a licensed vehicle 24 hours day and as such it is incapable of operating on purely private basis outside the licence see *Benson v Boyce* [1997] RTR 226 and *Yates v Gates* [1970] 2 QB 27; [1970] 2 WLR 593.

An alternative is to rely on existing controls to safeguard the public and to protect drivers and not to use CCTV.

Existing control measures include the requirement for Disclosure & Barring Service (DBS) checks for drivers upon application and then every three years. Incidents continue to be reported to Cheshire Constabulary despite these DBS checks.

The DBS check provides a snapshot at that time of categories such as unspent convictions, depending on whether a basic or enhanced check is undertaken. If an incident occurs after a successful check has been undertaken, this would not necessarily be picked up unless the organisation requested another DBS check to be undertaken.

Where the Council receives a complaint or allegation, it currently has no option but to suspend the driver pending an investigation. The implementation of CCTV would provide the council with the means to have a quicker overview of any alleged incident.

What enforcement activity is there?

The Council's Licensing Enforcement Team carry out periodic enforcement operations in conjunction with other partner agencies e.g. the Cheshire Constabulary, Trading Standards Officers, Benefits Fraud Officers and Vehicle Examiners at Network Warrington. These enforcement operations include, vehicle maintenance checks, airport checks on vehicles, benefit fraud checks and mystery shopping exercise i.e. for plying for hire, disabled access etc.

Consultation requirements
Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Consultation can be used at any stage of the PIA process.

Existing operators and licensing trade

The service has spoken with other authorities who have systems in operation .The service has consulted with the trade, approximately 575+ taxi and private hire drivers had been consulted, on the licensing policy, which includes the implementation of CCTV Policy and 4 responded to the policy, the feedback received was evaluated and put forward to the full licensing committee and Full Council for consideration and determination.

No privacy issues were identified prior to the adoption of the policy. The trade have subsequently raised concerns about the privacy of high profile clients and that of family members when the vehicle is used for private purposes. Representatives of the trade have asked for clarification on the intended benefit, why all drivers are required to comply rather than a case by case basis, the effect on their privacy and that of their family when the vehicle is used for domestic journeys, the intended retention period and the frequency of checks to ensure that the system remains operational.

Since the introduction of the Policy three drivers have raised concerns with the Information Commissioner (ICO), primarily relating to the proportionality of the recording when in personal use. The Council is continuing to liaise with the ICO and all drivers will be kept advised accordingly.

Elected Members

The introduction of the policy has been considered by both members of the Licensing Committee and Full Council, who approved the recommendation to adopt the policy.

Internal stakeholders

The service is continuing to work with appropriate internal stakeholders, such as Information Governance, ICT, and the Specialist Transportation Unit. The information governance team have been working closely with the ICT department to ensure that the solutions meet key information security standards such as PSN (Public Services Network) and legislation such as the Data Protection Act

The service continues to liaise with these areas and the Specialist Transport Unit to ensure continued compliance and to reduce risks to the drivers and passengers.

WARRINGTON
Borough Council

Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

How is the data collected?

- The CCTV systems record visual only from when the vehicle's ignition is turned on and for up to 15 minutes after the ignition is switched off.
- Sound can only be recorded when the driver feels he needs additional protection in the vehicle. The sound recording is only activated for 15 minutes. Drivers are advised to allow at least a 15-minute period to expire before taking a new passenger who is unrelated to the original incident.

How is the data stored?

- Data stored on hard drive for 14 days

How and when will data be removed?

Data will only be accessed/ removed for one of the following reasons:-

- To ensure operational integrity of the solution and the recording
- When there is evidence of a criminal offence
- When requested by police
- When there is a challenge to the 'fit & proper' standard
- When requested via a 3rd party as a DPA sec 29 or sec 35
- When requested as a Subject Access Request Please refer to Appendix C WBC CCTV download policy

Solution Integrity Checks

The Council's Licensing Section will carry out periodic quality checks on the integrity of the CCTV systems to ensure compliance. If any issues are identified the Licensing Officers will liaise with the CCTV Suppliers and Council's IT Section to resolve them.

WARRINGTON Borough Council

Privacy issues, related risks and solutions
Identify the key risks and the solutions that can be implemented to reduce the impact of each risk.

Accompanying guide can be used to help identify the DPA related compliance risks

Privacy issue	**Risk(s)** (refer to Appendix B)	**Solution(s)**	**Evaluation** (also need to state if the risk is eliminated, reduced or accepted)	**Approval/ Ownership?**
Excessive recording of members of the public in the vehicle	New surveillance methods may be an unjustified intrusion on their privacy. People may be concerned about the risks of identification or disclosure of information. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. Public distrust about how information is used can damage an organisation's reputation.	The system will automatically overwrite data after 14 days. Public are using a commercial vehicle which is used for public transport and would be expected to abide by the terms and conditions governing the use of the vehicle. Appropriate signage displayed advising of the use of CCTV. Exemptions considered for additional condition vehicles that carry passengers who require privacy.	The individual will be aware that they are using a commercial vehicle which is used for public transport and that they must abide by the terms and conditions governing the use of the vehicle. Signage will advise of the use of CCTV. The system has been installed to protect the public and as such the recording of the data is not considered to be excessive. The data will only be accessed by an appropriate officer in the event of a serious incident. The appropriate officer will use the WBC camera download policy. All other data will be automatically overwritten. The data stored is fully encrypted and held securely in a lockable safe in the Taxi Licensing Office. The public will be advised that they have a limited period in which to report the incident.	Dave Watson Regulatory Services Unit Manager

			In accordance with well-established case law all driving of a Licensed vehicle is regulated by the legislation and accordingly such vehicles cannot be used for personal use The measure is considered to be justified, compliant and proportionate on this basis. Please see information provided in previous sections.	
Intrusion from recording of members of the public outside the vehicle.	New surveillance methods may be an unjustified intrusion on their privacy.	There will be limited collateral intrusion outside of the vehicle as the camera will be positioned accordingly. Signage will be displayed on the vehicle which will be visible from the outside.	The cameras will be installed in a way that ensures that there will be minimal 'over spill outside of the vehicle. The risk is considered to be minimal. The measure is considered to be justified, compliant and proportionate on this basis. Please see information provided in previous sections.	Dave Watson Regulatory Services Unit Manager
Intrusion of recording of taxi drivers whilst working.	New surveillance methods may be an unjustified intrusion on their privacy. If a retention period is not established information might be used for longer than necessary. Non-compliance with the DPA or other legislation	The system has been installed to protect drivers who are using a commercial vehicle. The driver should be operating the vehicle in accordance with the terms and conditions of the licence. Data is encrypted. Data will only be accessed	Drivers are operating a commercial vehicle, which is used for public transport and must already abide by the terms and conditions of their licence. The data is encrypted and will be overwritten after 14 days. The CCTV system is designed to help to protect the welfare and integrity of the drivers.	Dave Watson Regulatory Services Unit Manager

	can lead to sanctions, fines and reputational damage.	securely in the event of an incident by approved and restricted staff		
Intrusion of taxi drivers whilst not working	New surveillance methods may be an unjustified intrusion on their privacy.	A licensed vehicle remains a commercial vehicle, used for public transport 24 hours a day. Data is encrypted. Data recorded whilst the vehicle is not working will not be accessed. Data will be overwritten after 14 days.	A licensed vehicle remains a commercial vehicle to be used for public transport 24 hours a day. The data is fully encrypted and data would only be accessed by an appropriate officer in the event of an incident. Only those images related to the incident will be accessed. All other data would be overwritten. There is no commercially available option to switch the system on and off as this would leave it open to abuse, which would result in uncontrollable risks.	Dave Watson Regulatory Services Unit Manager
Storage of data within the vehicle	Should the data be accessed it will display video images of passengers and driver for the previous 14 days(+). Data could be accessed and/or destroyed illegally to inhibit prevention/detection of	The data is stored within a secure unit. The data is encrypted	The data is stored within a secure, encrypted device, that only an appropriate officer can access where there is a clear and defined purpose	Dave Watson Regulatory Services Unit Manager

	crime. Data losses which damage individuals could lead to claims for compensation.			
Transfer of data to WBC device.	Unsecure transfer of data could impact on the validity of the data and lead to a DPA breach. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. Problems which are only identified after the project has launched are more likely to require expensive fixes.	The data will only be accessed in the event of an incident. It will only be accessed by an appropriate officer. The data will remain encrypted. It will be stored securely in line with the departmental policy for access and retention	The data will only be accessed in the event of an incident by an appropriate officer. The data will remain encrypted throughout the transfer. It will be stored securely on approved WBC systems with restricted access and appropriate data protection arrangements. In the event of an incident which requires the licensing team to view video, the taxi or private hire vehicle will be brought to the Council Offices for the licensing team to remove the relevant encrypted SD cards and replace and re-seal new cards into the MDVR. Taxi or private hire vehicle drivers must give the time and date of the incident to the licensing team so that the relevant video can be searched	Dave Watson Regulatory Services Unit Manager

			for on the SD card.	
Storage of data within WBC	Footage is not stored securely breaching the Data Protection Act 1998	Any data will be secured when stored in line with the departmental policy	The Council has a range of existing plans and policies in place to ensure that data is held securely.	Dave Watson Regulatory Services Unit Manager
Staff misuse of data	Footage access by staff without a defined purpose for access	The data will only be accessed by an appropriate officer and held securely. All staff have received training on data protection and security. The council has appropriate policies and procedures in place.	The Council has appropriate policies and procedures in place. Data will only be accessed by an appropriate officer for the purposes of detecting crime. The data will be stored securely.	Dave Watson Regulatory Services Unit Manager
Transfer of data and ownership to relevant partner.	Unsecure transfer of data could lead to a DPA breach and/or have a negative impact on an investigation.	The data will only be transferred where there is a need. Any request for access to the data for the purposes of detecting crime will be considered in accordance with a data sharing agreement.	Data will only be shared where it is appropriate to do so in accordance with data sharing agreements. Any request and subsequent decision to provide the data will be signed off by an appropriate senior officer.	Dave Watson Regulatory Services Unit Manager
Disposal of data.	Unsecure disposal of data could lead to a DPA breach. If a retention period is not	Data will be automatically overwritten after 14 days. Any data accessed and stored for the purposes of detecting crime and disorder will be kept in	The Council and the service have appropriate data retention policies in place. Any data that has not been accessed for the purposes of detecting crime and disorder will be	Dave Watson Regulatory Services Unit Manager

	established information might be used for longer than necessary. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.	accordance with existing policies of retention.	automatically be overwritten within 14 days.	
Wilful destruction of the data/unlawful access.	Inadequate disclosure controls increase the likelihood of information being shared inappropriately. Wilful destruction may prevent the detection of crime. Data not stored or disposed of in line with the Data Protection Act 1998 Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.	The data is held securely and cannot be accessed by the driver. Action can be taken under the conditions of the licence in the event that anyone attempts to interfere with the system. The council has disciplinary arrangements in the event of any misconduct by a member of staff	The system is held securely and the data is encrypted. Only an approved officer of the Council can access the system. Action can be taken under the terms and conditions of the licence. The Council has data protection and governance arrangements in place. Any wilful failure to abide by these procedures would be considered under the disciplinary process.	Dave Watson Regulatory Services Unit Manager

Drivers lack of buy in due to not seeing the benefits of the system	Drivers elect not to licence their vehicles with WBC, Increasing the number of non WBC/CCTV taxis operating in the area	Explicit communication to drivers about the identified risk factors and benefits of using CCTV as a deterrent and/or recording device	One of the primary concerns of drivers was one of cost. Steps have been taken to assist drivers in securing appropriate systems at a commercially competitive rate via a procurement framework. The Council and its strategic partners will continue to communicate with drivers, setting out the risks and the benefits of using a CCTV both in terms of crime, personal safety and market value/commercial benefit.	Dave Watson Regulatory Services Unit Manager
Drivers fitting their own CCTV outside of this process and having responsibility for the data and lack of corporate control over this	Warrington Borough Council having no control over the data recorded. This impact on subject access requests and affect the Council's reputation	Drivers holding a licence with Warrington Council will be required to install a compliant system. The implementation of the policy is expected to drive up standards within the trade and a number of local authorities are currently considering the benefits of CCTV	Drivers not licensed by Warrington Council may elect to fit their own system, which may not be deemed to be a fully compliant system. The driver would remain the asset owner, with full responsibility for their system. We liaise closely with neighbouring authorities and any intelligence on risks or emerging issues will be shared. We expect other authorities, and indeed drivers, to look at similar systems, of an appropriate standard, as the systems are installed and accepted.	Dave Watson Regulatory Services Unit Manager

WARRINGTON Borough Council

Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action	Status
Liaise with the Surveillance Commissioner regarding the PIA	January 2016	Sarah Gallear	Completed
Sign off of technical specification, including secure data transfer.	March 2016	Dave Gallear Sarah Gallear (for IG approval of secure data transfer)	Completed
Confirm the extent of the cameras field of view with respect to outside of the vehicle.	May 2016	Caroline Sharkey	Completed
Development of a protocol for accessing data and appropriate sign off/governance of the request	April 2016	Dave Watson in conjunction with the Information Governance Team	TBC?
Sign off data sharing arrangements and response to subject access requests.	April 2016	Information Governance Team	TBC?

Agree appropriate signage	April 2016	Caroline Sharkey	Completed
Agree data retention procedures.	April 2016	Dave Watson in conjunction with the Information Governance Team	TBC?
Agree secure data storage	March 2016	ICT	Completed
Agree process for considering business requests for exemptions.	February 2016	Caroline Sharkey	TBC?
Obtain internal approval and sign off, including information governance, IT and the monitoring officer.	April 2016	Sarah Gallear	Completed
Implementation	June 2016	All	Ongoing
Consultation with service users and taxi drivers over any ongoing issues.	Ongoing	Caroline Sharkey	Ongoing

Contact point for future privacy concerns:

Date PIA Completed:	**This version: 28/10/2016**
Reviewed by: **(Member of IG Team)**	**28/10/2016**
Approved for next step Y/N	**N/A In ongoing updates stage**
Approval Date:	

WARRINGTON Borough Council

Appendix B – Risks

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.
- Not recording at all times of a journey could impact on the comfort and safety of the passenger

Corporate risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Not recording and an incident occurring could have reputational damage and impact on internal and external investigations
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the DPA.
- Non-compliance with human rights legislation.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.

WARRINGTON Borough Council

Appendix C Taxi and Hackney Carriage Vehicles Camera Download Policy

The policy is as follows:

1. All passengers are made aware of the fact that they are being recorded by notices strategically placed on the vehicles. A minimum of 3 warning signs, approved by an authorised officer, must be clearly and prominently displayed inside the vehicle advising passengers that a CCTV system is in operation in the vehicle. These labels clearly warn that both audio and visual recordings take place in the vehicle using wording and images of a camera and a microphone (Audio recording will only be permitted for use where the driver believes it is in the interest of his or a passenger's safety or for the purpose of protecting his livelihood. The driver will be advised to allow the 15-minute period to expire before taking a new passenger who is unrelated to the original incident) The labels displayed will also inform passengers that audio recording will only be activated use where the driver believes it is in the interest of his or a passenger's safety or for the purpose of protecting his livelihood

2. Data will only ever be downloaded 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 a substantive complaint has been made to the licensing authority regarding a specific vehicle / driver and that complaint is evidenced in writing (and cannot be resolved in any other way),

   (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 the Data Protection Act.

3. To safeguard the data all downloads will be conducted in the presence of at least two relevant people. Relevant people are: a member of the Warrington Borough Council (WBC) licensing team or a serving police employee. This will generally be at the Council offices with two Licensing staff and a Police Officer where possible.

4. All requests must be in an appropriate format detailing the powers that allow the release of the data and providing all the information required. The request form for download must state the approximate time of the event/occurrence and only the timescale relevant to the specific incident will be downloaded, decrypted and thereafter stored.

5. On receipt of a download request to be conducted by WBC staff an authorised member of the Licensing Team will confirm it is a legitimate request. If practical, arrangements will be made with the owner of the licensed vehicle for the vehicle to attend the Licensing Office. If it is not practical then an authorised member of the Licensing Team will attend the location of the vehicle or data box to facilitate the download. Any download will be carried out in the presence of at least one other person if at the licensing office. If the download is taking place away from the licensing office then either an additional member of Council staff or a member of the requesting organisation i.e. police officer will be present in addition to the member of staff conducting the download.

6. A dedicated computer will be used to facilitate the download from the data box. This computer will copy the downloaded footage onto its files. A master copy will be created from this computer and placed on the external hard drive dedicated for such use and retained by WBC Licensing Team. This hard drive will be kept secure to prevent loss of data. A working copy will be produced and either given to the requesting authority or subject or retained by the investigating officer. Data retained by WBC Licensing Team will only be retained for the following periods:

   a. Cases leading to prosecution 10 years from date of trial
   b. Formal caution 3 years from date of caution
   c. Written warning or no formal action 3 years from date of decision
   d. Subject Access request 6 years from date of request.

   The file on the dedicated computer will be deleted once the master and working copies are produced.

   Staff in the Licensing Team will conduct a review of material held on the hard drive each year in March and erase any such material outside of these time limits. Any working copies should be placed on the appropriate files and they will be weeded and safely destroyed with the files whose time limits mirror those set out above.

7. Data will only be viewed by the person performing the download to the extent necessary to facilitate the download process. Data being used in any investigations will only be viewed by persons involved in that investigation but will be released to be used in court if necessary.

8. After a period of time any data held by the system installed in any vehicle is automatically overwritten dependant upon the specification of the system installed. Typically, this will be within a period of 14 days.

9. Only systems approved by the Licensing Team may be installed by an approved installer – thereby ensuring that any equipment may not be tampered with, encryption is of a sufficient standard and data may not be interfered with or released to any third party / published.

Appendix D POLICY ON CCTV SYSTEMS IN VEHICLES LICENSED BY WARRINGTON B H COUNCIL

WARRINGTON
Borough Council

Licensing Section, Regultion and Protection,Warrington Borough Council, New Town House, Buttermarket Street, Warrington,Cheshire,WA1 2NH

Telephone: 01925 442517 or Email: taxj@warrjngton,goy,uk

Generalpolicy

1. This policy applies to private hire, additionally conditioned private hire and hackney carriage vehicles (referred to as "vehicles").

2. The Licensing Authority will maintain an approved list of CCTV systems, which it has approved for installation in vehicles in accordance with this policy. Any individual or organisation may apply for any system to be placed on the approved list, however only those systems which meet the Minimum System Specification [see below] would normally be approved.

3. With effect from 1st June 2016 vehicle proprietors must, upon application for a new licence or for renewal of a current licence, as part of that application, install in the vehicle a CCTV system which appears on the Licensing Authority's approved list.

4. Upon installation, such vehicle licences will be subject to additional conditions to ensure that such CCTV systems are appropriately installed and maintained so as not to interfere with the safety and comfort of passengers, as well as ensuring the integrity of any images captured.

5. This policy details the minimum standards that will normally be expected to be met before a CCTV system will be placed on the Licensing Authority's approved list.

6. This policy should be read in conjunction with the attached guidance notes, which outline the application procedure, to be followed by an individual or organisation who wishes to obtain approval for a CCTV system, as well as from proprietors who wish to install such systems in their vehicles.

7. Whilst each case will be determined on its own merit the Licensing Authority will normally only place on its approved list CCTV systems which meet or exceed the Minimum Specification contained in this policy.

If you have any specific queries regarding the CCTV Policy then please do not hesitate to contact the Licensing Team on the above number or e-mail us,

Minimum System Specification

The following are the minimum criteria that the Licensing Authority would expect a CCTV system to meet in order for the system to be placed on the list of CCTV systems approved to be installed in vehicles. The system shall, as a minimum:

- Meet the current Information Commissioner data protection requirements.
- Be capable of date & time system identification stamping.
- Be capable of recording and storing images for a minimum period of fourteen days.
- Be capable of capturing images that, in low light conditions, must be of sufficient quality to enable identification of any person travelling in the vehicle and be of such quality that they can be used for prosecution purposes.
- Be capable of storing images in a manner, which prevents them being removed, downloaded or viewed by the driver or any other person travelling in the vehicle.
- Provide that images are only capable of being downloaded by authorised officers of the Licensing Authority.
- Provide that images are digitally encrypted. De-encryption software required to view the recorded images must be supplied to the Licensing Authority free of charge before the system is installed in the vehicle.
- Provide that the hard disk or data card is not able to be accessed by the driver or any other person travelling in the vehicle.
- Provide that the data unit is stored separately from the camera(s) and out of view of person travelling in the vehicle.
- Provide that cameras are capable of being fitted in locations that do not affect the safety of any person travelling in the vehicle, and located as securely and discreetly as possible to avoid passengers travelling in the vehicle from tampering with them.
- Provide that, where the system uses a DVD recorder, the system is protected from shock.
- Any system must be marked with the EMC [Electro Magnetic Certification], which signifies that it meets the European Industry Standard.

If you have any specific queries regarding the CCTV Policy then please do not hesitate to contact the Licensing Team on the above number or e-mail us.

- Provide that activation of the system shall be via the vehicle's ignition system (or alternative method approved by the Licensing Authority) and that recording shall continue 15 minutes after the ignition is switched off. The system will not be provided with any other on/off mechanism that is accessible to the driver or any passenger.

- The system must have the facility to default to not recording audio. Audio recording will only be permitted for use where the driver believes it is in the interest of his or a passenger's safety or for the purpose of protecting his livelihood.

Application Process for a CCTV system to be approved by the Licensing Authority

1. An individual or organisation who wishes to apply to the Licensing Authority for the approval of a CCTV system must apply in writing (email is acceptable) for a particular make and model of CCTV system to be placed on the approved list.

2. The applicant must provide evidence that the product complies with the Licensing Authority's minimum recommended specification.

3. Once the system has been approved the Licensing Authority will issue the applicant and the manufacturer (where the manufacturer is not also the applicant) written confirmation, and include the system on the approved list. If the system is not approved the Licensing Authority will issue the applicant notification of the same and the reasons for the decision.

4. System approval will be required for each new product or any modification to an existing approved product.

Conditions to be attached to private hire, additionally conditioned private hire and hackney carriage vehicles

1. No CCTV system shall be installed in a vehicle unless it has previously been approved by the Licensing Authority.

2. The number and location of all cameras must be declared to the Licensing Authority. The number and location of cameras shall not be varied without the prior written consent of the Licensing Authority.

3. A minimum of 3 warning signs, approved by an authorised officer, must be clearly and prominently displayed inside the vehicle advising passengers that a CCTV system is in operation in the vehicle. The notices shall be positioned in a prominent (though not obstructive) position where they can be easily read by persons both inside and outside of the vehicle. 1 warning sign for front seat passengers and 2 for rear seated

If you have any specific queries regarding the CCTV Policy then please do not hesitate to contact the Licensing Team on the above number or e-mail us.

passengers. The proprietor shall ensure that the notices are maintained in a clean and legible condition.

4. The proprietor shall ensure that the system is properly and regularly maintained and serviced in accordance with the manufacturer's instructions. Written records of all maintenance and servicing shall be made and retained by the proprietor for a minimum of 12 months. Such written records shall be made available on demand by an authorised officer of the Licensing Authority.

5. Upon request for image retrieval by an officer of the Licensing Authority or a police officer the proprietor shall ensure that the CCTV system is made available to the officer as soon as reasonably practicable, and in any event within 7 days of the request.

6. The proprietor of the vehicle shall take all reasonable steps to ensure that any driver of the vehicle is made aware of every condition in relation to any installed CCTV system and has been given adequate instruction regarding the need for the system to be made available as soon as reasonably practicable, and in any event within 7 days of any authorised request for any image retrieval.

If you have any specific queries regarding the CCTV Policy then please do not hesitate to contact the Licensing Team on the above number or e-mail us.