



Data Protection Impact Assessment (DPIA)

Template and Guidance

Data Protection Impact Assessment for:	CCTV in Licensed Vehicles
Information Asset Register Reference:	IAR

Version	Date amended	Amended by	Changes
1	20/07/2018	Dave Watson	
2	30/08/2018	Dave Watson	Amended to include further information on the options considered.
3	01/04/2019	Vicky Simcott	Amended to reflect audio trigger function, data retention and GPS

Initial screening to identify if you need to complete a DPIA

If you select yes to any below, you will need to complete the whole DPIA form

Question	Y/N
Will the project involve the collection of new information about individuals?	Y
Will the project compel individuals to provide information about themselves?	Y
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	Y The Project involves the use of CCTV in licensed vehicles, however the use of CCTV in



	general is now common place.
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Y
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 private.	Y
Will the project require you to contact individuals in ways that they may find intrusive?	N



The Data Protection Impact Assessment Full Template

Step 1: Identify the need for a DPIA

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.

Purpose

Legal basis.

CCTV is integral to the effective licensing and regulation of hackney carriage and private hire vehicles under the Local Government (Miscellaneous Provisions) Acts 1976 and 1982 and Town Police Clauses Act 1847 and 1875 as amended from time to time. This places a responsibility on the Licensing Authority to protect the public by ensuring that only safe and suitable people hold a licence to carry passengers.

The Council is subject to a variety of duties prescribed by legislation, Government Guidance and circulars to protect the public and to prevent and detect crime and to keep children and vulnerable adults safe . Examples are the Children Act 2004 which requires the Council to carry out its functions with regard to the need to safeguard and promote the welfare of children and the Care Act 2014 which prescribes a general duty to protect vulnerable adults from abuse and neglect.

Legislation setting out the duties and powers requiring the council to have regard to safety, crime and disorder, antisocial behaviour includes (but is not limited to) the following legislation (as amended or modified):

- Local Government Act 1972
- Local Government Act 2000
- Local Government (Miscellaneous Provisions) Acts 1976 and 1982
- Children Act 2004
- Care Act 2014
- Crime and Disorder Act 1998
- Criminal Justice and Public Order Act 1998
- Equality Act 2010

Evidence can be provided to the Police under the provisions of the Police and Criminal Evidence Act 1984.

Other Law Enforcement Agency (LEA) such as HM Revenue & Customs; HM Border Force and services within the Council such as Trading Standards and Environmental Crime would also have the necessary criminal investigatory powers to request CCTV footage as under statutory legislation or via the gateway under Data Protection Act 2018.

There is a legitimate need to protect drivers and the travelling public and to deter and detect crime. The Council considers it necessary to process data when the vehicle is being used in a licensed capacity under the Local Government (Miscellaneous Provisions) Act, and that it cannot reasonably achieve the same purpose without CCTV being operational.



There are six available lawful bases for processing under the Data Protection Act 2018 (DPA 2018), The Council recognises that these are of equal importance. CCTV is there to assist the Local authority in complying with the regulatory function and to detect and deter crime and, in extreme situations, to protect life, however, the Council does not seek to rely on vital interests for the purpose of processing data and will be processing the information under Article 6 of the GDPR: Lawfulness of processing: 1.Processing shall be lawful only if and to the extent that at least one of the following applies:- (e) 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 controller.

A description of the typical operation of a CCTV unit is provided in Appendix 1.

The use of CCTV in a licensed capacity is considered to be necessary and proportionate for the purposes of:-

Purpose	Lawful basis
Protecting drivers when working in a licensed capacity.	Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
Performing the local authority function of determining the safety and suitability of licensed drivers	Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
Protection and reassurance of the travelling public	Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
Protection of vulnerable people who rely on taxis as an essential means of transport	Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
Deterring and detecting crime in the public interest	Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

What alternatives are there to the proposed solution?

Document if there is anything, what you have considered and reasons why the proposed solution is the most appropriate option.

No CCTV capability

A number of crimes have been reported to the Council and requests made for CCTV evidence. The range of offences are set out in figure 1. There is anecdotal evidence from officers that there have been a significant increase in requests for evidence from the Police since the introduction of CCTV for the purposes of detecting crime. In order to protect the integrity of any ongoing criminal investigation it is not always possible to receive updates on the progress of cases but the Police will pass on information upon conviction where there is a risk to the public. Civil and criminal action may also be taken under the Local Government (Miscellaneous Provisions) Act and the Town Police Clauses Act by the Licensing Authority if the driver is alleged to have committed an offences. Further action can be taken by the Licensing Authority if the conduct of the driver falls below that set out in the Driver Code of Conduct in the Taxi policy and they are judged not to be a fit and proper person to hold a licence.

FIGURE 1: Nature of incident relating to the CCTV download request.

REDACTED: Breakdown of incident type by volume

here is a clear basis in law from which to process the data for the purposes of protecting the driver and the travelling public. Furthermore, CCTV is integral to the effective licensing and regulation of hackney carriage and private hire vehicles under the Local Government (Miscellaneous Provisions) Act; when the vehicle is being used in a licensed capacity.

A significant proportionate of drivers, some 40%, are from an ethnic background. This increases the likelihood of hate crime and racial abuse. This is evidenced in Figure 1.

CCTV helps to reassure the travelling public particularly those that 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 requirement. Whilst the majority of offences are committed against the driver the risk to passenger safety can also be evidenced within the emerging CCTV data in Figure 1.

The introduction of CCTV allows the Council to work with the Police, trade, taxi marshals and street pastors to direct people towards vehicles which operate to the highest standards of public safety in that they have operational CCTV installed. This gives the passenger increased choice as operators may be licensed by other Councils who do not operate to similar standards. The Council is the sole data controller. Please see the next section on data sharing.

The availability of CCTV increases the fear of sanction and reduces 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. This increases the likelihood of securing an appropriate sanction, helps to ensure that the victim receives appropriate restitution, and reduces the risk posed. **CCTV provides a legitimate means of deterring and detecting crime.**

The potential consequences of not having a continual means of detecting crime could be very grave in the event of a serious incident. We will seek to assist the Police in their investigations where it is appropriate to do so under the Police and Criminal Evidence Act 1984 or Data Protection Act 2018

gateway. We would also seek to assist other Law Enforcement Agencies (LEA) who have conduct of criminal investigations where it is appropriate to do so under specific legislation or are able to make a request under the Data Protection Act 2018 gateway.

Where the Council receives a complaint or allegation relating to an incident within the cabin of the vehicle, it currently has little or no option but to suspend the driver pending an investigation. The implementation of CCTV provides the council with the means to have a quicker overview of any alleged incident. This is of benefit to the driver as the allegation can be investigated in a timely, proportionate and effective way.

The Council cannot solely rely on DBS as these only provide a snapshot in time. Incidents have arisen across the country where drivers with no previous convictions, or who comply with the convictions policy have committed offences. The Police are also only currently required under the data sharing agreement to provide evidence upon conviction to the Licensing Authority. The Council has a legal obligation under the Local Government (Miscellaneous Provisions) Act to protect the travelling public, and a decision may be required for this purpose prior to the outcome of any criminal conviction, which carries a higher legal threshold than that required for the purposes of the Local Government (Miscellaneous Provisions) Act, in ensuring that the driver remains a fit and proper person at all times.

The footage and audio (where activated) from the DVR is only accessed where there is a legitimate purpose to do so and is **not** subject to constant monitoring and is **not** downloaded unless there is a lawful reason for doing so under public task basis (Article 6 :1e) for processing data under the DPA 2018. This will be limited to the downloading of data for a defined period only where an alleged crime has occurred; an offence under the Local Government Miscellaneous Provisions Act, an offence under the Town Police Clauses Act; a Subject Access request has been received, a safeguarding incident has been reported or where a complaint has been received alleging a breach of the driver Code of Conduct, or to check the date stamp on the device and to check that it remains operational (this will only be done for a period of time when the vehicle is being used for non-private use and when no passengers are present in the vehicle).

A parallel system to record when the driver 'clocks' on and off duty and to audit such a system is not required. The Council would not use the system for the purposes of monitoring when the driver is working or otherwise. The Council would instead rely on the bookings taken by the operator to cross reference whether the vehicle was been used in a licensed capacity at the time of the incident and/or witness statements and the facts of the case.

The analysis of the data download requests has also shown that a significant number of incidents have occurred against drivers and that it is not possible to predict when these incidents are likely to occur. CCTV forms a legitimate means of protecting drivers. It also serves to act as a deterrent.

Warrington Borough Council has determined that:-

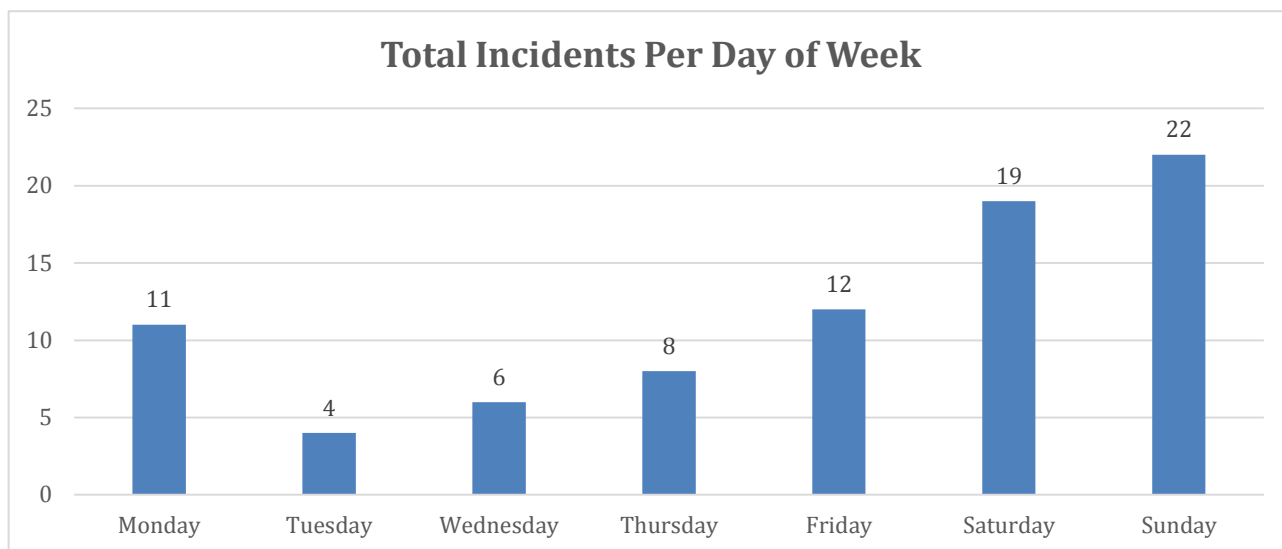
- It has a lawful basis for processing personal data to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- CCTV is integral to the effective licensing and regulation of hackney carriage and private hire vehicles under the Local Government (Miscellaneous Provisions) Act.
- There is a legitimate need to protect drivers and the travelling public and to deter and detect crime.



Default off position unless the system is activated

An analysis of the data downloads to date, where there has been a legitimate reason to do so, has shown that there is no standard incident, or victim profile, from which to reasonably predict the likelihood of an incident occurring with an appropriate degree of confidence. This option has been discounted as it does not provide an acceptable level of protection.

FIGURE 2: Total CCTV incidents per day.



Whilst a number of incidents do occur at the weekend this also coincides with peak demand. It can however be evidenced from the data in Figure 2 that 35% of the incidents occur outside of the weekend period (Friday-Sunday). This is a significant proportion of the incidents given the risk.

It can be seen from the information in Figure 3 that a number of incidents of a serious nature still occur outside of peak demand, which introduces unacceptable risks if CCTV was not operational, when the vehicle is being used in a licensed capacity at these time.

Alternatives were considered as was the possibility of having no CCTV in vehicles. Private hire operators maintain records of bookings but the recording of a booking, whilst helpful, does not assist sufficiently in crime prevention or detection or safeguarding purposes. Similarly, passengers may use their personal mobile phones to record incidents but this is not reliable and does not safeguard adequately. Drivers should not be using mobile phones whilst driving. The integrity of images/recordings made by individuals may be questioned and is dependent upon their being made in stressful circumstances. This does not offer sufficient protection.

Reliance upon verbal or written accounts after the event is not reliable and not a viable alternative. Reliance upon town centre CCTV is inadequate as it will not record the inside of a moving vehicle and has limited coverage.

Figure 3: Nature of CCTV incident according to day.

REDACTED: Breakdown of incident type by day of the week.

Figure 4: TOTAL CCTV incidents per time of day.

REDACTED: Incident by time of day

The absence of continuous recording when the vehicle is being used in a licensed capacity would fail to provide an appropriate level of safeguarding for the following minimum reasons:-

- The driver may not have sufficient warning to predict the likelihood of an incident occurring, e.g. cases of sudden assault from behind, or making off without payment.
- It may be unsafe for the driver to try to urgently activate the system whilst driving.
- It is not considered to be an appropriate alternative solution to locate the switch within the cabin. The driver would therefore need to leave the vehicle in order to activate the system. This is not likely to be practical in the event of an incident.
- Incidents have occurred where the driver has been accused of an offence. The systems may not be activated, meaning that CCTV evidence would not be available.
- CCTV is there to protect the vulnerable and to protect the travelling public. The passenger would need to be familiar with the correct operation of any activation method. Vehicles are also used by vulnerable groups who may not have the time, mental or physical capacity to quickly activate the system. A separation activation from that used by the driver would be required. This does not provide an appropriate level of safeguarding for the passenger. Serious incidents reported include sexual assault, indecent exposure and inappropriate behaviour towards the passenger.
- Incidents have arisen where the passenger has allegedly been involved in crime, we have also had incidents of missing persons in licensed vehicles. The driver would be unaware of the risk and would not activate the system.
- Incidents have arisen where the driver has committed a littering offence, or a passenger has alleged that they have been injured as a direct result of the traffic incident involving the way the vehicle was being driven.
- The passenger may make an allegation against the driver, which is unfounded. The absence of CCTV would mean that the subcommittee need to consider the case on its relative merits, in the absence of in cab CCTV footage, which may result in the driver being suspended or having their license revoked.

System with an alternative override location

Systems are equipped with a manual override for use when the vehicle is being used in a non-licensing capacity. The system is located outside of the cabin and in the boot. The following alternative locations have been considered and are not considered to be the most appropriate solution:-

- (a) **Override system under the bonnet:** There is significant potential that the system will be unduly affected by heat and it will not be sufficiently isolated from vibration and debris. The engine bay is not a safe working environment from which to access data when the vehicle has been running for a period of time.

Override switch within the cabin: The system would potentially safeguard against inadvertent deactivation by use of a double action switch, or a system where the switch must

be depressed for a period of time. However, incidents have been reported alleging inappropriate behaviour, indecency, assault and sexual assault by the driver. The location of a switch within the cabin would not adequately safeguard the public in these serious situations. The likelihood of which cannot be reasonably predicted. The drivers still have the option to manually override the system when the vehicle is in private use. It is a requirement of the licence to have operational CCTV when used in a licensed capacity. The availability of an override switch in the cabin would make enforcement of the condition difficult as drivers would be able to quickly reactivate the system during a spot check by enforcement. The only alternative means of enforcement would be to access the data and to check the system log. However, this would require a random 'sample' of the data to be accessed even when no offence may have been committed. Officers need to have the ability to quickly check that the system is operational using the system warning lights to make enforcement practical, to minimise any intrusion, and to minimise any unnecessary interference with the continued use of the vehicle in a licensed capacity. Whilst it is a condition of their licence to have operational CCTV when the vehicle and driver are working in a licensed capacity, the driver may become reliant on only activating the system when they feel that an incident is likely to occur. This is inequitable with the fair use of the system to protect the passenger. Furthermore, it may fail to adequately protect the driver themselves from sudden assault or incidents of an unpredictable nature.

Not to require any run on time after the ignition is used to switch the main live power feed off.

The CCTV system is there to protect the travelling public and vulnerable users of taxi vehicles as well as drivers. There have been allegations of assaults by drivers of a physical and sexual nature and allegations of inappropriate behaviour. Incidents of this nature may occur when the vehicle is stationary with the engine off. The CCTV system takes a live feed from the ignition. This would allow the system to be deactivated by the driver, without the knowledge of the passenger, by using the vehicle ignition switch. This would fail to provide an appropriate level of safeguarding for the passenger.

The absence of a run on time would also enable any potential perpetrator to use the ignition as a means of deliberately deactivating the recording when the vehicle is being used in a licensed capacity for the purposes of committing crime, or for breaching the conditions of their licence.

This would be possible if the system did not operate with a separate live feed taken from the battery, as the ignition switch would provide the sole source of power.

A separate live feed is therefore taken from the battery to enable the system to remain operational for a limited defined period; after the engine is switched off via the ignition. This is common practice in the industry and is often specified by local authorities for the purposes of detecting and deterring crime. This provides an appropriate level of safeguarding and protection of passengers, whilst allowing any incident occurring after the vehicle is stationary with the engine off to be investigated.

Once the system is configured in this way, it would not be possible to override the system using the manual override switch located in the boot of the vehicle, as this would need to be moved to the 'off position' before first activation of the ignition and use of the vehicle. This ensures that the system remains operational for a limited period for the legitimate reason of protecting drivers and the travelling public and for the purposes of deterring and detecting crime, under public task, and providing evidence of alleged offences from LEAs.

Modern vehicles are fitted with stop/start systems, which would mean that the systems would not be active during periods when the start/stop system is used, unless the CCTV system is configured to allow it to continue to record for a limited period.

Incidents have also occurred where the driver has left the vehicle. The ability of CCTV to record whether the driver is or is not present in the vehicle has helped to support cases where it can be proven that the driver has left the vehicle for the purposes of committing an offence. This can help to corroborate witness statements and help to place the driver at the scene of the offence.

The Council considers it necessary to process data when the vehicle is being used in a licensed capacity under the Local Government (Miscellaneous Provisions) Act, and that it cannot reasonably achieve the same purpose without CCTV being operational after the ignition is turned off for a limited period.

To specify a shorter run on time after the ignition is used to switch the main live power feed off.

A 30 minute period is typically specified by other local authorities. The system specification for Warrington is for the system to continue to record for a limited 15 minute period only after the ignition is turned off.

This is considered to be necessary based on our experience of the likely nature of the incident, its likely duration, and the need to protect drivers and passengers. Incidents can occur when the vehicle is stationary. These include arguments that result in an assault on the driver, racial abuse, threats, and making off without payment. It is important that we are able to collate sufficient evidence for the purposes of the lawful investigation of any offence under enactment. The council must also ensure that the driver remains a fit and proper person to hold a licence under the provisions of the Local Government (Miscellaneous Provisions) Act.

There is no typical incident profile from which to determine the likely occurrence of an incident and the likely duration of an event with any degree of confidence. Indeed, incidents may escalate over a period of time. A breakdown of incidents and an estimated duration is provided in Figure 5.

Figure 5: Typical durations of incidents involving CCTV.

REDACTED: Incident type by typical duration of the incident.

The 15 minute run on period is used for the legitimate purpose of safeguarding both the passenger and the driver and for detecting crime.

The driver does not have the option to select an alternative 'run on time' for this reason, the software also needs to be configured; making it impossible for the alternative time periods to be selected without a full update to the software. Alternative time periods of between 3 mins to 15 minutes have been considered. These have been discounted based on the risk of incidents occurring and lasting for longer than 15 minutes. Officers have estimated from a review of the download requests received to date that incidents can last for over 15 minutes. A shorter period is not considered to provide an appropriate level of safeguarding. Increasing the risk of a serious crime occurring and the risk that there is no corroborating evidence to support the witness statement from the passenger, or indeed to prove the innocence of the driver in the event of a

malicious allegation being made.

The period has therefore been carefully specified to balance the legitimate lawful use of the system to and protect the privacy of the driver when the vehicle is subsequently used in a private capacity when the ignition is turned off, such as taking a break in the vehicle.

The driver still has the option to manually override the system prior to the first use of the vehicle if the vehicle is to be used in a non-licensing capacity. Once the CCTV system has been activated and used in a licensing capacity the driver would need to allow a maximum of 15 minutes to expire before using the vehicle in a non-licensed capacity. This would mean that the driver must allow 15 minutes at the end of their shift before private use. No actual data would be accessed for this period as there would be no legitimate reason to do so. In the event that the driver wished to take an immediate break after taking a passenger they have the option of taking their break outside of the vehicle, or waiting for the expiry of the 15 minutes. When balanced against the legitimate need to protect the driver and the travelling public this is not considered to be unreasonable or an excessive intrusion of privacy.

A shorter run on time after the ignition has been switched off has been discounted as it would fail to adequately protect the travelling public, the detection and deterrence of crime and would undermine the effective licensing and regulation of hackney carriage and private hire vehicles under the Local Government (Miscellaneous Provisions) Act.

System without audio capability

It is a requirement of the Technical Specification to have audio capability on the CCTV system.

System with audio capability with standard recording time or system trigger.

It is considered to be an excessive invasion of privacy to continually record conversations in a licensed vehicle. The Technical Specification therefore requires a system trigger to be installed to record audio in the event of an incident. The audio must only be activated in the event of an incident occurring. The system will return to normal non-audio default operation within a short period of time (approximately 3-5mins depending on supplier configuration). The recording period can be extended by using the system trigger to reactivate the system, however, this should only be done if the incident continues beyond the default period. The provision of a system trigger minimises the risk of excessive recording and has been specified for this reason. It allows the driver to take another passenger after the incident and upon completion of default recording period due to the short period(s) of time the audio can be activated for. The system indicators will show when the audio has been activated and when the system has returned to the default of no audio recording.

This solution was selected as there has been evidence of racial abuse and inappropriate behaviour, whilst the vehicle is being used in a licensed capacity and because it is considered to be both necessary to perform a task in the public interest or for official functions, and because there is a lawful basis to do so. It enables evidence to be obtained to investigate an offence under the Police and Criminal Evidence Act and to take action where necessary under the Local Government (Miscellaneous Provisions) Act.

CCTV recording with no capacity to override.

This has been discounted to balance privacy requirements.

Access Requirements (who will have access, how, when etc.)

Will anyone external to the Council need access? How will this be managed

The Council will act as the sole Data Controller. The Council will only access the data where it has a legitimate purpose to do so. The data will automatically overwrite after a maximum of 30 consecutive days. The data is held in an encrypted format using encryption software that meets or exceeds the current FIPS 140-2 (level 2) standard or equivalent. The system is held securely within the vehicle and it cannot be accessed remotely.

The installer will only be able to view live footage during installation or maintenance. The vehicle will not be occupied by either the driver, or indeed any passenger during these periods.

The data is encrypted and only the data required for the legitimate purpose for which it is needed will be downloaded, e.g. the period of the alleged incident. Random checks will be carried out to ensure that the system is set to the correct date and time to reduce the risk of accessing the incorrect footage. This will be done for times when the vehicle is not being used in a private capacity and for which there is no passenger.

Only authorised staff will be trained and have access to the software necessary to complete the download. We currently have two members of the Public Protection Team who have received training on the use and operation of the system. All staff must complete mandatory data protection training. Other members of the Public Protection Team may be nominated as authorised staff to ensure that a limited number of officers are available and trained to access any footage in the event of an incident being reported and staff being on leave. A CCTV Download Request form will be completed, which will record the officer who has authorised the download and the officer performing the download and the outcome.

Only the required period on the date stamp will be downloaded. The data will be held on a standalone encrypted laptop, which will be stored securely in the Council offices and it will only be capable of being accessed by an authorised officer. The original data held on the CCTV system within the vehicle will be automatically overwritten after a maximum of 30 days incident and data downloaded will be deleted after 14 days in accordance with the retention period.

Over 80% of download requests to date have been made by the Police for the purposes of investigating a criminal offence under the Police and Criminal Evidence Act. Requests have also been received from Warrington Borough Transport following an assault on a travel assistant; Warrington Borough Council Public Protection officers for the purposes of investigating littering offences under the Environmental Protection Act 1990 and alleged breaches of Warrington BC's Taxi Policy.

The processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

All law enforcement agencies (LEA), including the police, will be required to complete a download request form. The authorising WBC officer will then carry out an assessment of the request to



ensure that there is a legal gateway to request the data and the request is consistent with the CCTV policy for release of data. The CCTV Request Download Form will be retained to show the decision making of the authorising officer and the outcome of the download itself. This will only record if footage was or was not downloaded; the time length of the downloaded footage; if a copy was provided to the LEA; and date of removal of the CCTV from the standalone laptop.

Any subject access requests received from data subjects will be processed in line with the Council's subject access request procedure. As part of the validation of the request, we would require copies of identification to be provided. In order to provide the information, the Council may need to ask for further information or clarification to help identify the time period relating to the data subject. As part of the process we would also consider whether any other data subjects feature and whether there is a requirement to pixelate aspects of the footage. This would be reviewed on a case by case basis.

Step 2: Describe the information flows

The collection, use and deletion of personal data should be described here. It may 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 records visual only from when the vehicle's ignition is turned on and for a specified period of time after the ignition is switched off. The driver has the ability should they wish to, to manually deactivate the system in the event that the licensed vehicle is used in a private capacity.

Sound/audio can be recorded when the driver or passenger feel that they need additional protection in the vehicle if an incident occurs. The system is configured to only record sound for a short period of time once activated to ensure that it does not record excessively and so that new passengers can be taken without risk of intrusion. Data is not accessed remotely. In the event of an incident and where there is a legitimate reason to do so under the public task the period of the incident only will be 'collected' from the CCTV system in the vehicle. The data will remain encrypted throughout this process.

GPS data is being continually collected to ensure that the time and date stamp of recorded data is accurate. GPS location information is available but would only ever be accessed if there was a legitimate and justified reason for accessing the location of the vehicle.

The driver will be requested to present the vehicle to the Council offices by agreement.

How is the data stored?

Data is stored on the hard drive within the vehicle for a minimum of 14 consecutive days and a maximum of 30 consecutive days, the data is then automatically overwritten. The data is encrypted and is configured in a way that it can only be accessed by authorised officers. All captured images must be protected using encryption software that meets or exceeds the current FIPS 140-2 (level 2) standard or equivalent. Authorised officers are WBC Public Protection Staff who have received training on the system. All staff have received mandatory data protection training. The Council only currently has two authorised officers for this purpose but more maybe authorised to ensure that there is sufficient



operational cover in the event of an incident.

When is the data accessed?

Data will only be accessed/ removed by an authorised officer where there is a legitimate reason to do so for one of the following reasons:-

- To ensure operational integrity of the solution and the recording,
- Where a crime report has been made involving the specific vehicle and a LEA have formally requested the data,
- When a substantive complaint has been made to the licensing authority regarding a specific vehicle / driver,
- Where a data request is received from an applicant 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,
- When requested as a Subject Access Request. Please refer to Appendix C WBC CCTV download policy.

The CCTV system is held securely in the vehicle and is fully encrypted to FIPS 140-2 (level 2) standard or equivalent. The Technical Specification requires the analogue and digital ports to be deactivated to prevent access by the driver or any person travelling in the vehicle. The storage unit must be concealed from view and be provided with a download port for access by WBC authorised personnel. The download port is only accessible to authorised officers of the Council who have a legitimate reason to access the system using a unique key to the unit. The data is encrypted in accordance with the Technical Specification.

The method of data download is determined by the technical specification of the camera system installed; these fall in to two categories; download achieved via cable connection between the recording device and an encrypted standalone laptop or removal of the SD card or HDD from the recording device and the SD card inserted in to the encrypted stand-alone laptop to download the footage or HDD inserted into HDD reader and into the stand alone laptop to download the footage.

The data is downloaded in an encrypted format onto a standalone laptop installed with specialist software from which to view the appropriate footage. The data download will be restricted / limited to the period specified on the Authorised Download Request form and each request will be assigned a unique reference number. The data remains encrypted throughout the process. The technical specification makes provision for the data to be provided in a standard DVD video format, suitable for playing on a PAL format region 2 player. Should the download footage be required to be produced in a format that the requester can take away as evidence in an investigation the download footage will be burnt to a DVD. This will be issued to the requester with the downloading officer witness statement and the requesting officer will need to sign for receipt of the evidence.

The installer will only be able to access 'live' footage at an appropriate and agreed location, when there is no driver or passenger in the vehicle, and the vehicle has been presented by the driver for system installation, upgrade, or maintenance check.

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. The integrity check will be limited to a

period when the vehicle is being driven to the compliance check where there are no passengers and that it was not being used in a private capacity. The checks will be carried out as part of targeted operations depending on intelligence and operational need. It is typically envisaged that approximately 4 operations will be carried out per annum, subject to intelligence and the availability of resources.

Data Retention

The CCTV technical specification requires that the data is held on the CCTV unit in an encrypted format to FIPS 140-2 (level 2) standard or equivalent for a minimum of 14 days. It is considered that depending on the use of the vehicle and the capacity of the hard drive there could be up to a maximum of 30 days of data. The 14 day period has been selected as this is considered to be the minimum period in which an incident can be reported, investigated, a download request made, an assessment of the legitimate reasons or otherwise of that download request made, the vehicle made available and the data secured. This period minimises the period of data processed for performing a task in the public interest, or for official functions, and where the task or function has a clear basis in law.

Data will only be downloaded to the standalone encrypted, access restricted laptop where a Download Request Form has been received by the Council and the request authorised. The encrypted data on the laptop will only be retained for a period up to 14 days after the release of the data to ensure that it viewed by the investigating body. The encrypted file will then be deleted from the laptop. The 14 day period is considered to be a sufficient period of time in which to check that the evidence is admissible.

The Data Protection Act 2018 (DPA) gives individuals the right to require access to personal data (subject access request). The Council has procedures for responding to any SAR. In the event that a SAR is received, and the data can be legitimately secured within the 14 day retention time, then the requester will be provided with a copy of their personal data, in accordance with the Council's procedures and the ICO's code of practice. The encrypted data will be deleted from the standalone laptop within 14 days of the data been provided to the requestor. This is considered to be a reasonable period of time to ensure that the requestor can view their personal data before the original encrypted copy is deleted from the system.

No data downloads of the original encrypted data will be made and the standalone laptop is not networked for this reason.

Action in the event of wilful destruction of the data/unlawful access by Council Staff

It is important to set out from the outset that staff continue to work in a professional and responsible way to protect the public and to ensure that they comply with the terms and conditions of their contract, and the various legal requirements placed upon them. All staff have received data protection training. The Council has appointed a Data Protection Officer and Senior Information Risk Owner.

Additional steps have been protect to safeguard against unauthorised access to the data and any wilful destruction of data outside of normal procedures governing retention.

The system specification requires that the system will store images in a manner which prevents them from being removed, downloaded, or viewed by the driver or any other person travelling in the

vehicle. The system must also ensure that images can only be downloaded by authorised officers of the Council. These are officers within public protection who have received training on the correct use of the system. Again these officers will have also completed the corporate data protection training. There are only currently two authorised officers but more may be trained to ensure that there is sufficient operational capacity to access images, where there is a legitimate reason to do so within the 14-30 day retention period of the system, after which the data will be automatically overwritten. The systems vary but access is typically via a cable connected to a download port. The encrypted data can only be accessed using specialist software stored on a secure laptop which also has encryption and password protection. Any SD card is held securely within the CCTV unit, behind a secure panel, which requires a key to access. The key is held securely with limited access by authorised officers.

The technical specification requires that the system has an internal log to record access to the system. This cannot be accessed by the authorised officer and is held indefinitely by the system, unless and until any routine maintenance of the system by the supplier. The supplier must notify the Council in advance of any maintenance or reformatting of the system that would affect data retention to ensure that no data, as a result of an incident, is destroyed before it can be secured as evidence.

In the highly unlikely event that any evidence is wilfully and deliberately destroyed by an authorised officer, then this will be investigated in accordance with the Council's Disciplinary Policy. Appropriate action would then be taken having regard to the circumstances of the case. Any breach of the Data Protection Act 2018 would be investigated by the Information Governance Team as part of their standard incident process and where an incident met the appropriate criteria, would be reported by the Data Protection Officer to the ICO.

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 prior to the original adoption of the Policy (2014-16).

The service consulted with the trade, approximately 575+ taxi and private hire drivers were consulted, on the licensing policy, which included the implementation of CCTV Policy and 4 responses to the policy were received.

No privacy issues were identified prior to the adoption of the policy by Full Council following consideration by the Licensing Committee.

The information governance team were involved in the original DPIA and process including responding to any concerns raised after the consultation process.

Consultation on the latest Policy (2018).


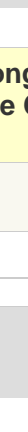

The Council consulted widely on the updated policy including with the trade, an open consultation on our website, public notice and with other neighbouring authorities and interested parties. **No**



privacy issues were raised. There have also been recent press releases in relation to the use of CCTV in the local newspaper. No comments or adverse comments have been received directly by the Council by the travelling public. There is some anecdotal evidence received by elected members that the public welcome the additional safeguarding. Whilst the response to the website consultation was low, an excerpt is provided below.

CCTV Systems in Hackney Carriage/Private Hire Vehicles

12. To what extent do you agree or disagree with the proposed changes to the revised CCTV Policy? Please select one option.

		Response Percent	Response Total
1	Strongly agree		20.00% 1
2	Agree		60.00% 3
3	Neither agree or disagree		20.00% 1
4	Disagree		0.00% 0
5	Strongly disagree		0.00% 0
Analysis	Mean: 2	Std. Deviation: 0.63	Satisfaction Rate: 25
	Variance: 0.4	Std. Error: 0.28	
			answered 5
			skipped 1

13. If you disagree / strongly disagree, can you please give a brief explanation as to where and how, in your opinion, the CCTV policy sections should be made clearer or changed in the box below

		Response Percent	Response Total
1	Open-Ended Question		0.00% 0
No answers found.			
			answered 0
			skipped 6

Consultation with the trade.

The Council has consulted widely on the updated policy including a number of consultation events with the trade. This included a detailed letter sent to all of the Council's taxi/private hire licence holders (approximately 1,413 licence holders) to inform them of the changes. In addition, a notice was published in Warrington Guardian newspaper, a dedicated consultation webpage was created on the Council's Taxi Licensing website, Council Officers attended a meeting with one of the large private hire operators in Warrington, the taxi/private hire trade were invited to attend a consultation event on 13th March 2018 and an open day was held on 24th April 2018 at the Town Hall.

This has, along with the fact that the Policy has been in place since 2016, helped the vast majority of drivers and operators to better understand the benefits of CCTV and the Council's policy. Two drivers have continued to raise concerns about privacy.

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. The updated policy was approved and adopted by Licensing Committee on 12th June 2018.

Internal stakeholders

The CCTV policy was considered at Licensing Committee and approved at Full Council. A wide range of internal stakeholders have been consulted as part of the policy development, including: Information Governance (Data Protection Officer), ICT, the Specialist Transportation Unit, legal services, finance, procurement and communication

External stakeholders

We continue to work with the Cheshire Constabulary and we have been liaising with other authorities, suppliers and the Local Government Association to promote best practice.

Privacy and the ICO

Three drivers raised concerns with the ICO, at the outset of the policy, which resulted in an investigation. No additional privacy issues have been raised by other drivers. No new privacy issues have been raised.

The Council has corresponded with the ICO on this issue and has committed to using less intrusive alternatives to protect privacy, specifically the ability for drivers to temporarily deactivate the system when the vehicle is being used in a private capacity. The Council is committed to working with the ICO policy team to develop and promote best practice.

Step 3 & 4: Identify 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) Includes risk to individuals and the organisation	Solution(s)	Result:- is the risk is eliminated, reduced or accepted)	Evaluation: - is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
<p>Excessive recording of members of the public in the vehicle</p>	<p>People may be concerned about the risks of identification or disclosure of information.</p> <p>Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.</p> <p>Public distrust about how information is used can damage an organisation's reputation.</p>	<p>The system will automatically overwrite data after a maximum of 30 consecutive days.</p> <p>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.</p> <p>Appropriate signage displayed advising of the use of CCTV.</p> <p>Exemptions considered for additional condition vehicles that carry passengers who require privacy.</p>	<p>The risk is reduced to an acceptable level.</p>	<p>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. Each vehicle is required to display signage to show that it is a licensed vehicle.</p> <p>Additional signage will advise of the use of CCTV. The signage includes a QR code where the individual can find out further information.</p> <p>The system has been installed to protect the public and as such the recording of the data is not considered to be excessive.</p>

		<p>The policy has been in place since June 2016. It has attracted significant publicity. No adverse comment or objection has been provided by a member of the public in relation to its use or by a passenger.</p>	<p>The passenger does not have the capability to request that the CCTV be deactivated as this would be contrary to the conditions of the licence and would increase the risk to the driver.</p> <p>There is also no audio unless it is specifically activated by the driver, and this will only record for the duration of the incident. Provision has been made in the Technical Specification for a trigger to activate the system. If installed this should be accessible to the driver and the passenger.</p> <p>The data will only be accessed by an authorised officer in the event of a serious incident.</p> <p>The authorised 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</p>
--	--	--	--

				<p>have a limited period in which to report the incident. (See previous information in the DPIA).</p> <p>The measure is considered to be justified, compliant and proportionate on this basis.</p>
<p>Intrusion from recording of members of the public outside the vehicle.</p>	<p>People outside of the vehicle are concerned about any inadvertent recording and intrusion on their privacy.</p>	<p>There should be no collateral intrusion outside of the vehicle as the camera will be positioned to focus recordings on the cabin and the system requirements specify how this should be minimised.</p> <p>The system installer is required to specify that the system has been correctly installed and a certificate of installation is provided to the data controller.</p> <p>Signage will be displayed on the vehicle which will be visible from the outside.</p> <p>Compliance checks will look at camera alignment and coverage.</p>	<p>The risk is considered to be minimal.</p>	<p>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.</p> <p>The measure is considered to be justified, compliant and proportionate on this basis.</p>

<p>Intrusion of recording of taxi drivers whilst working.</p>	<p>Drivers may feel that it is an unjustified intrusion on their privacy.</p> <p>If a retention period is not established information might be used for longer than necessary.</p> <p>Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>The system has been installed to protect drivers who are using a commercial vehicle.</p> <p>The driver should be operating the vehicle in accordance with the terms and conditions of the license.</p> <p>Data is encrypted to FIPS 140-2 (level 2) standard or equivalent.</p> <p>Data will only be accessed following the receipt of a completed CCTV Download Request Form which has been reviewed and the download authorized by a Principal Officer; the Licensing Manager or Head of Service. The data is not constantly monitored, accessed or downloaded.</p>	<p>The risk is considered to be minimal.</p>	<p>Drivers are operating a commercial vehicle, which is used for public transport and must already abide by the terms and conditions of their license. The data is encrypted and will be overwritten after 14-30 consecutive days. The CCTV system is designed to help to protect the welfare and integrity of the drivers.</p> <p>The DPA (article 6 of the GDPR (c) allows for the lawful processing of data for the exercise of any functions conferred on any person by or under enactment.</p> <p>The legitimacy of the goals of public protection and prevention and detection of crime are integral to the effective licensing and regulation of taxis.</p>
--	--	--	---	--

<p>Intrusion of taxi drivers whilst not working</p>	<p>Drivers may feel that there is an unjustified intrusion on their privacy.</p> <p>Drivers may be fearful of being recorded when the vehicle is being used in a private capacity.</p> <p>Drivers maybe fearful of using the vehicle for private use once the ignition has been switched off, as the system continues to record data for 15mins.</p> <p>A policy maybe disproportionate if it fails to consider alternative means increasing the risk of sanction.</p>	<p>Data is encrypted to FIPS 140-2 (level 2) standard or equivalent.</p> <p>The Council as the sole Data Controller will never access the data unless it has a legitimate reason to do so. This is highly unlikely when the vehicle is being used in a private capacity minimising the intrusion.</p> <p>Whilst a licensed vehicle remains a licensed vehicle at all times it is acknowledged that some drivers may elect to use it in a private capacity. All drivers have been given the option of temporarily overriding the system whilst the vehicle is used in a private capacity.</p> <p>In order to detect crime and to provide an appropriate level of safeguarding the CCTV unit will continue to record for 15mins after the ignition in turned off, a rationale for this period has been provided in previous sections of the DPIA.</p> <p>Data will be overwritten after 14-30 consecutive days.</p>	<p>Reduced to an acceptable level.</p>	<p>The final approach is considered to be proportionate in that the Council has considered alternative means (please see the section of the DPIA on alternative solutions) to limit any deliberate misuse of the system, whilst providing drivers the ability to temporarily deactivate the system whilst in private use.</p> <p>The 15min ‘run on’ after ignition is there it protect the interests of drivers and their passengers, to deter the deliberate use of the ignition as a means of quickly deactivating the system for the purposes of committing an offence, and to enable an appropriate amount of evidence to be gathered in the event of an incident. The period has been carefully selected to allow for a sufficient degree of safeguarding and protection, whilst allowing the vehicle to be used in a private within a reasonable period of time.</p>
--	--	---	---	--

<p>Storage of data within the vehicle</p>	<p>Should the data be accessed it will display video images of passengers and driver for up to 30 days.</p> <p>Data could be accessed and/or destroyed illegally to inhibit prevention/detection of crime.</p>	<p>The data is stored within a secure unit.</p> <p>The data is encrypted</p> <p>Only the authorised officers of the Council have access to the data.</p> <p>The data storage will not be accessible by the driver or the passengers.</p>	<p>Reduced to an acceptable level.</p>	<p>The data is stored within a secure, encrypted device, that only an appropriate officer can access where there is a clear and defined purpose.</p>
<p>Transfer of data to WBC device.</p>	<p>Unsecure transfer of data could impact on the validity of the data and lead to a DPA breach.</p> <p>Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>The data will only be accessed where there is a legitimate reason to do so.</p> <p>The officer will complete a download assessment to ensure that the download if necessary, proportionate and that any collateral intrusion is eliminated or minimised.</p> <p>Only the date and time range required for the legitimate use will be accessed. The date and time are checked as part of a regular process to ensure that they are recording accurately.</p> <p>It will only be accessed by an authorised officer.</p>	<p>Reduced to an acceptable level.</p>	<p>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 standalone laptop with restricted access and appropriate data protection arrangements. (Please see previous sections of the DPIA on accessing data).</p> <p>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.</p>

		The data will remain encrypted. It will be stored securely in line with the departmental policy for access and retention.		Only the data range necessary to gather evidence in relation to the alleged incident or SAR will be accessed.
Storage of data within WBC	Footage is not stored securely breaching the Data Protection Act 2018	Any data will be secured, stored and destroyed in line with the departmental retention policy. The data will be stored separately from the main server on a standalone laptop, with secure restricted access. This will be stored securely with limited access. (Please see detailed comments in the DPIA on storage and retention). No backups of the data will be taken.	Reduced to an acceptable level.	The Council has a range of existing plans and policies in place to ensure that data is held securely.
Staff misuse of data (Please see the specific section in the DPIA).	Footage access by staff without a defined purpose for access	The CCTV system has an internal access log for traceability. The log cannot be altered by the authorised officer and the log will be retained in the system memory indefinitely, or until the system is maintained. The supplier must notify the Council of any maintenance that would affect the memory of the device.	Reduced to an acceptable level	The Council has appropriate policies and procedures in place. Data will only be accessed where there is a legitimate reason to do so under public task. The data will be stored securely and deleted in accordance with the section of the DPIA on data retention.

		<p>The data will only be accessed by an authorised officer and will be held securely.</p> <p>The officer is required to complete a download assessment and a record is maintained of who has accessed the system and for what purpose. The assessments are stored in the sections case management system, which has been set up to limit access to named officers only.</p> <p>All staff have received training on data protection and security. Authorised officers have also received training on the correct use and operation of the CCTV software.</p> <p>The council has appropriate policies and procedures in place.</p>		
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.	Following receipt of a CCTV Download Request Form from a LEA and the completion of the download of the footage the requesting LEA may require the footage to be produce in a format they can take away for evidential	Reduced to an acceptable level	Data will only be shared where it is appropriate to do so in accordance with the DPIA.

		<p>purposes. Should this be required the LEA then become the data holder and sign to confirm they take on the responsibilities to hold the data securely; only use it for the requested purpose and to dispose of it when it is no longer required as evidence. Each CCTV Download Request received is allocated a URN and all communications and action in respect of the download are recorded in a data management system with access restricted to officers authorized from CCTV download under the Scheme of Delegation of Officers Powers.</p> <p>These are stored on a document management system with restricted access.</p>		
--	--	--	--	--

<p>Disposal of data.</p>	<p>Unsecure disposal of data could lead to a DPA breach.</p> <p>If a retention period is not established information might be used for longer than necessary.</p> <p>Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>Data will be automatically overwritten on the CCTV system held securely in the vehicle after a maximum of 30 days.</p> <p>Any data accessed and stored for the purposes of detecting crime and disorder will be kept in accordance with existing retention policies and for no longer than is necessary.</p> <p>The data is not constantly viewed or downloaded and will only be accessed for a legitimate purpose.</p>	<p>Reduced to an acceptable level</p>	<p>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 automatically overwritten after a maximum period of 30 days.</p> <p>14 days is considered to be a reasonable period in which to report crime, to make a legitimate access request for information. (please see the section of the DPIA on accessing the data and data storage and retention) and to download the data and to ensure that it is no kept for longer than is necessary on the internal memory of the CCTV system.</p>
---------------------------------	---	--	--	---

<p>Wilful destruction of the data/unlawful access.</p>	<p>Inadequate disclosure controls increase the likelihood of information being shared inappropriately.</p> <p>Wilful destruction may prevent the detection of crime.</p> <p>Data not stored or disposed of in line with the Data Protection Act 2018</p> <p>Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>The data is held securely and cannot be accessed by the driver.</p> <p>Action, such as the suspension, or revocation of the license can be taken under the conditions of the license in the event that anyone attempts to interfere with the system.</p> <p>The system has an internal log and full traceability in terms of access. The authorised officer cannot amend the system log. The log will be retain indefinitely or until the system is maintained. The supplier must obtain approval from the Council before any work is carried out that will affect the system memory.</p> <p>The council has disciplinary arrangements in the event of any misconduct by a member of staff</p>	<p>Reduced to an acceptable level</p>	<p>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 license.</p> <p>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.</p> <p>The officer is required to complete a download assessment justify access and use of the data, which is held securely.</p>
---	--	---	--	---

<p>Drivers lack of buy in due to not seeing the benefits of the system</p>	<p>Drivers elect not to licence their vehicles with WBC, Increasing the number of non WBC/CCTV taxis operating in the area</p>	<p>The policy requirement has been in place since 2016.</p> <p>There has been no observed drop off in renewal of applications or new applications.</p> <p>The vast majority of drivers support the use of the system.</p> <p>The Council has continued to consult on its policy.</p>	<p>Reduced to an acceptable level</p>	<p>The vast majority of drivers support the policy. The Council has upgraded the systems to address the concerns that have been raised.</p> <p>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.</p>
<p>Drivers fitting their own CCTV outside of this process and having responsibility for the data and lack of corporate control over this</p>	<p>Warrington Borough Council having no control over the data recorded. This impact on subject access requests and affect the Council's reputation</p>	<p>Drivers holding a licence with Warrington Council will be required to install a compliant system.</p>		<p>The Council is working with the LGA to promote best practice.</p> <p>The council has elected to upgrade systems.</p> <p>Drivers are required to install systems that comply with the technical specification.</p>

Step 5: Approval and sign off of DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
<p>Excessive recording of members of the public in the vehicle</p>	<p>The system will automatically overwrite data after 14-30 consecutive days.</p> <p>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.</p> <p>Appropriate signage displayed advising of the use of CCTV.</p> <p>Exemptions considered for additional condition vehicles that carry passengers who require privacy.</p> <p>The policy has been in place since June 2016. It has attracted significant publicity. No adverse comment or objection has been provided by a member of the public in relation to its use or by a passenger.</p>	<p>Dave Watson, Public Protection Unit Manager</p>
<p>Intrusion from recording of members of the public outside the vehicle.</p>	<p>There should be no collateral intrusion outside of the vehicle as the camera will be positioned to focus recordings on the cabin and the system requirements specify how this should be minimised.</p>	<p>Dave Watson, Public Protection Unit Manager</p>

	<p>The system installer is required to specify that the system has been correctly installed.</p> <p>Signage will be displayed on the vehicle which will be visible from the outside.</p> <p>Compliance checks will look at camera alignment and coverage.</p>	
Intrusion of recording of taxi drivers whilst working.	<p>The system has been installed to protect drivers who are using a commercial vehicle.</p> <p>The driver should be operating the vehicle in accordance with the terms and conditions of the license.</p> <p>Data is encrypted.</p> <p>Data will only be accessed securely in the event of an incident by approved and restricted staff</p>	Dave Watson, Public Protection Unit Manager
Intrusion of taxi drivers whilst not working	<p>Data is encrypted.</p> <p>Whilst a licensed vehicle remains a licensed vehicle at all times it is acknowledged that some drivers may elect to use it in a private capacity.</p> <p>All drivers have been given the option of temporarily manually overriding the system whilst the vehicle is used in a private capacity.</p>	Dave Watson, Public Protection Unit Manager

	<p>The period of time when recording continues after the engine has been switched off has been limited to 15mins.</p> <p>Data will be overwritten after 14-30 consecutive days.</p>	
Storage of data within the vehicle	<p>Any data will be secured, stored and destroyed in line with the departmental retention policy.</p> <p>The data will be stored separately from the main server on a standalone laptop, with secure restricted access. This will be stored securely with limited access.</p>	Dave Watson, Public Protection Unit Manager
Staff misuse of data	<p>The system logs access for traceability.</p> <p>The data will only be accessed by an appropriate officer and held securely.</p> <p>The officer is required to complete a download assessment.</p> <p>All staff have received training on data protection and security.</p> <p>The council has appropriate policies and procedures in place.</p>	Dave Watson, Public Protection Unit Manager
Transfer of data and ownership to relevant law enforcement agency.	<p>The data will only be transferred to another LEA when a CCTV Download Request has been completed by the LEA; the request authorized and the downloaded footage is required as</p>	Dave Watson, Public Protection Unit Manager

	<p>evidence.</p> <p>The third party is required to sign for an acknowledge receipt and assume responsibility for its safe use and destruction.</p>	
Disposal of data.	<p>Data will be automatically overwritten after 14-30 consecutive days.</p> <p>Data downloaded to the stand alone laptop will be deleted after 14 days from download. This is sufficient time to allow the requesting LEA to determine if the footage is required as evidence and to check that any downloaded footage supplied on DVD can be viewed.</p> <p>Footage on DVD supplied to LEA's will be retained in accordance their policies.</p>	Dave Watson, Public Protection Unit Manager
Wilful destruction of the data/unlawful access.	<p>The data is held securely and cannot be accessed by the driver.</p> <p>Action can be taken under the conditions of the license in the event that anyone attempts to interfere with the system.</p> <p>The system has an internal log and full traceability in terms of access.</p> <p>The council has disciplinary arrangements in the event of any misconduct by a member of</p>	Dave Watson, Public Protection Unit Manager

	staff	
Drivers lack of buy in due to not seeing the benefits of the system	<p>The policy requirement has been in place since 2016.</p> <p>There has been no observed drop off in renewal of applications or new applications.</p> <p>The vast majority of drivers support the use of the system.</p> <p>The Council has continued to consult on its policy.</p>	Dave Watson, Public Protection Unit Manager
Drivers fitting their own CCTV outside of this process and having responsibility for the data and lack of corporate control over this	Drivers holding a license with Warrington Council will be required to install a compliant system.	Dave Watson, Public Protection Unit Manager

Step 6: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA 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?

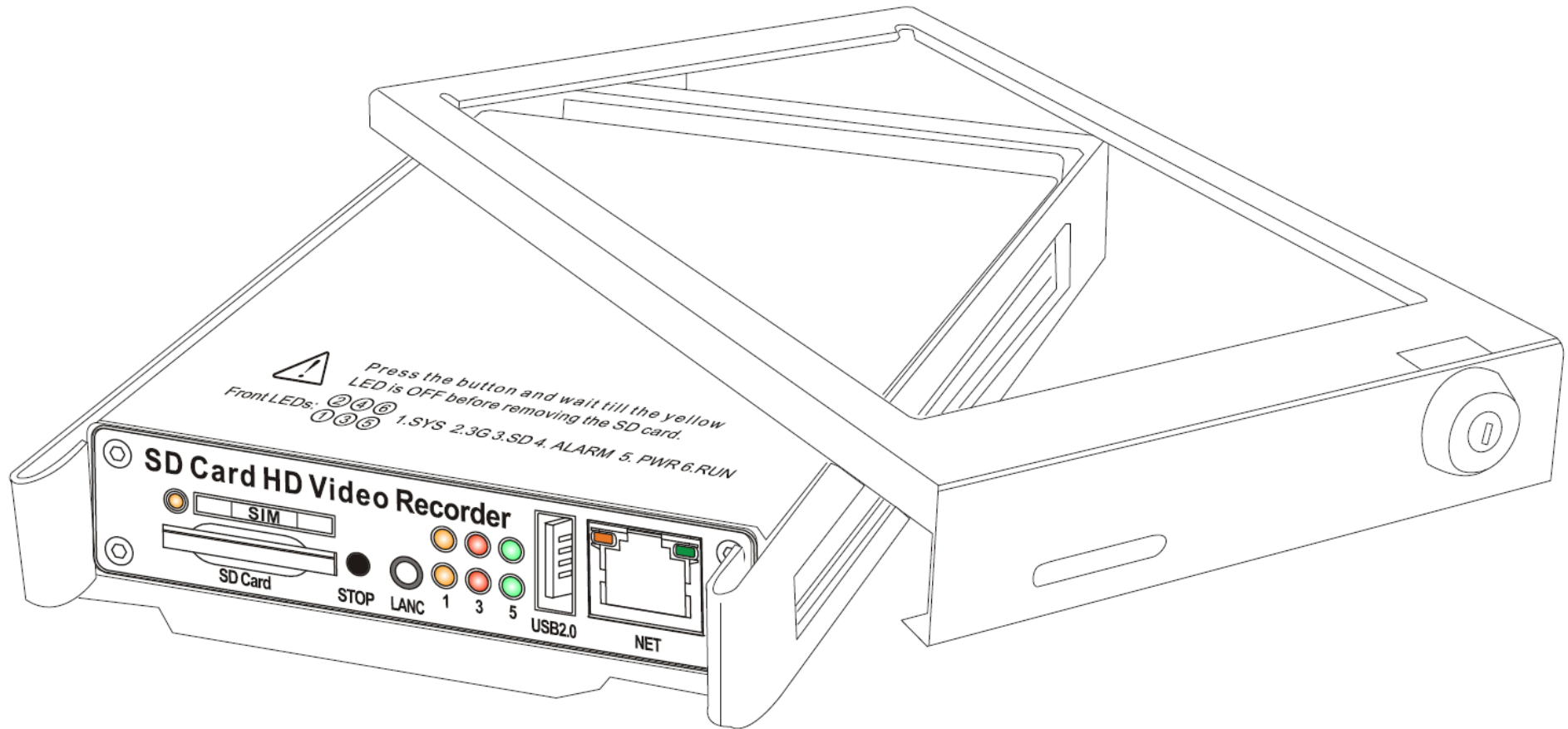
Action to be taken	Date for completion of actions	Responsibility for action
<ul style="list-style-type: none"> To continue to work with the ICO to promote best practice and to finalise the agreed approach. 	September 2018	Dave Watson, Public Protection Unit Manager
<ul style="list-style-type: none"> To complete the review of supporting Technical documents. 	September 2018	Dave Watson, Public Protection Unit Manager
<ul style="list-style-type: none"> To complete the tender exercise for CCTV systems 	October 2018	Dave Watson, Public Protection Unit Manager
<ul style="list-style-type: none"> To obtain Licensing Committee approval for the new policy. 	June 2018	Dave Watson, Public Protection Unit Manager
<ul style="list-style-type: none"> To update and replace existing systems in accordance with the Technical Specification 	Jan 19	Dave Watson, Public Protection Unit Manager
<ul style="list-style-type: none"> To work with the LGA to promote best practice 	December 18	Dave Watson, Public Protection Unit Manager

Contact point for future privacy concerns:

Manager Regulation & Protection, Warrington BC, New Town House, Buttermarket Street, Warrington, Cheshire WA1 2NH Tel: 01925 444051

Date DPIA Completed:	
Reviewed by: (Member of IG Team)	Sarah Gallear
Approved for next step Y/N	
DPO aware Y/N?	Yes
Approval Date:	
Next review date for information asset owner	

Appendix 1: Typical CCTV unit and operation. Please note that there is significant variation between products. All products must comply with the Council's latest Technical Specification.



GENERAL INTRODUCTION

The HDVR series mobile digital video recorder is a compact, full-featured H.264 1080p/720p recording system that uses a SD card as a storage device. The recorder unit and associated accessories are specifically designed for operation in a mobile environment. The HDVR system, used in conjunction with the

cameras, records up to four channels of full-motion video and audio data to a Class 10 (minimum) SD card. The firmware-driven menu system provides a simple method for configuring the unit's operation as well as searching for and viewing previously recorded AV records.

Product Main Features

- Embedded operating system, assuring reliability and system integrity.
- Records up to four channels of full-motion colour video with corresponding audio tracks.
- H.264 High Profile video compression.
- Total Record resource up to 120 1080P frame/second.
- Lockable security enclosure.
- Front panel USB2 port for recording to a flash card as an optional storage device.
- Ignition sense that provides DVR power-on in recording mode when the bus is started.
- Power-off delay record when the bus is shut-down with operator-selected delay times.

Video And Audio

- H.264 High Profile video compression, real time recording 1080p30, 720p30 and 540p30 for each channel. Frame rate adjustable for each channel.
- Audio compression:16bit 48KHz AAC codec. This codec offers high compression with high quality audio.
- 1080P resolution for each channel, which means each channel support 1920x1080 @30fps.
- Support 4 channel real time 1080P video and 4 channel audio recording.
- Real time live HD video and audio through WiFi, support Windows, Android and iOS
- Recorded HD video and audio real time playback over WiFi

5 -

Power Management

- Reliable power management, wide voltage: +8V~+32VDC; The power input is protected against short positive transient (1500 watts peak pulse power capability with a 10x1000 us waveform); The power input is protected against negative voltage. Applicable for vehicles with +12V or +24V battery.
- The recorder provides each camera with stable +12V DC power; DVR can detect the short cut on power circuit.
- DVR can monitor battery voltage after Ignition off, and auto into sleep mode when voltage is bellow specified level.