Northamptonshire Police
Data Protection Impact Assessment (DPIA) Stage 1

Project Title: CCTV from Mobile enforcement vans

You should start to fill out this template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Author	Department	Information Asset Owner	Project Manager
C0717 Matt O'Connell	Safer Roads Team	SUPT Jen Helm	BAU

Version	Version Date	Requester of change	Summary of change
1.0	15/04/2021	C0717 Matt O'Connell	Document creation
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
To enhance the evidence collected by the mobile enforcement vehicles, some of the fleet have been fitted with a bespoke 360 degree camera system. These cameras are linked to the Home Office type approved speed detection device and allow additional angles of footage to be recorded and timestamped alongside the main evidential recording. The cameras are placed on both sides of the van and to the front, this alongside the enforcement camera feed to the rear of the vehicle allows a near 360 degree field of view. The footage is used to support prosecutions detected by the operator, most notably recording the registration of motorbikes which do not have a front VRM. It is also used to provide reassurance to the operator when people approach the vehicle from their blind side. This type of processing sits within Law Enforcement and is used in line with the prevention and detection of crime.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

There are two versions of the system in operation, both have largely the same camera setup and capabilities. The main difference between them both is the data retention and automatic weed periods.

The system will be activated once the enforcement vehicle has reached an enforcement location and the equipment is being setup. Whilst on, the system records on multiple camera feed and stores this data on a hard drive within the system.

At the end of an enforcement session, if an offence is detected and additional footage is required to support the prosecution, the operator will export this from the system either onto a DVD or flash stick. This would then be exhibited and follow the main enforcement exhibit for processing.

At the processing stage, any additional still frames are captured from the exhibit to support the prosecution. For example, we would normally capture 3 images for a basic speeding offence. For a motorbike, we would capture;

- Offence image where the speed detection took place,
- Closer image of the rider,
- A final image of the VRM from this additional camera system.

The first two images would have been taken from the main enforcement exhibit.

The exhibited footage would be kept alongside the main enforcement session and disposed of in line with the MOPI guidance.

The footage stored on the system which is fixed into the enforcement vehicle is subject to an automatic weed. One of the systems weeds at 30 days and requires a password for access, the other at 72 hours however, it is not password protected.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The data is a multi-camera video feed which records vehicles passing the enforcement point and any pedestrians in close proximity of the van. The data would also include the feed from the enforcement camera, so would have speed reading overlays on one of the files. Each week approximately 120 hours of footage is captured. However, very little of this is processed further as described. Footage will potentially include Special Category and the very nature of the tool is to capture offence data as it happens. Only enforcement data will be retained, all other data will be disposed of through automatic weeding. The footage stored on the system in the enforcement vehicle is subject to an automatic weed. One of the systems weeds at 30 days and requires a password for access, the other at 72 hours however, it is not password protected. The enforcement vehicles operate across the County at designated enforcement locations. The number of data subjects whose data will be collected is unmeasurable, majority will be disclosed of but the numbers retained will be dependent on the level of non-compliance shown on the day. All data retained for law enforcement will then be disposed of in line with MoPI.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Individuals / vehicles recorded by the system are either offenders or passing members of the public. They would have no control of being recorded if they were to pass the enforcement point. The use of speed enforcement cameras is well known by the public and regular engagement is held through social media sites allowing access to information and to make views known. Majority of the counties of residents are in support of speed enforcement to improve the safety of the county. The data collected will include that of children and vulnerable groups but will only be retained where an offence has been committed. This is not a new or novel reason for processing. Speed enforcement cameras have been in use for a significant period of time. Northamptonshire Police acknowledge and refer to the 12 principals of Surveillance Camera Code of Practice and the ICO's CCTV Code of Practice. Code of practice - A guide to the 12 principles (publishing.service.gov.uk) 12_principles_diagram_v3.pdf (publishing.service.gov.uk) CCTV code of practice (ico.org.uk)

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The cameras are used as a method of detecting offences which impact on road safety. The system allows for the best evidence to be captured along with other offences which would not be able to be processed without this evidence. Evidence captured by the system is used to support prosecutions and reduce the number of those Killed or Seriously injured on our roads. Publicity of the use of the system also increases public confidence that these other offences are not being ignored on our roads.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
This camera system is a standard addition to the enforcement system used by forces nationally. Its use has been heavily publicised and has been met with support. Enforcement locations are identified for a number of reasons such as; • Collision hot spots • Community concern requests (supported by speed data collection) • Event / location specific sites (Modified car meets, Silverstone, Santa Pod) All locations are considered for their proportionality and transparency and are publicised online.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis for processing is the prevention, investigation, detection or prosecution of criminal offences. The processing of this information allows us to provide best evidence and bring offenders to justice. The system is only activated during enforcement periods and at specific locations. The enforcement vans have a CCTV warning sign with contact details for further information. All operators are trained in the use of the system and the data weed process is automated. To ensure adequate safeguarding and minimise intrusion on the public, enforcement locations are considered and created to ensure the cameras are not recording into private areas or dwellings. All internal transfers of data are recorded in statement form to protect the evidential chain of the data. The data is protected and there is no function for operators to delete evidence prior to the automatic weed process.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Loss of data confidentiality through unauthorised access to the system	Remote	Significant	Low
Capturing images of vehicles not being investigated for offences by the system	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Loss of data confidentiality through unauthorised access to the system	Restricted access to the vehicle Passworded system only shared with trained staff	Reduced	Low	Yes
Capturing images of vehicles not being investigated for offences by the system	Automated weeding ensures that data is kept for long enough to identify offences and then the rest of the data disposed of.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	T Kightley-Jones 23/11/2021	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The collection of data through mobile enforcement vans has been in place for a significant period of time and has not been the subject of data breach to date. It has undoubtedly been subject to complaint and questioning but has not cause to question the relevance or proportionality of its use. Additional cameras have caused us to refresh our consideration, particularly around our storage and transfer of data from the van systems onto force network. There are two separate camera systems in operation within these vans. The footage stored on the system which is fixed into the enforcement vehicle is subject to an automatic weed at 30 days and is password protected. The other system has a 72 hour retention and is not password protected. Both systems require manual transfer of data from van to our networked systems. There is some risk in this process however it should take place within a secure site and will involve limited data which requires further actions to be taken to identify individuals. The greater risk is that it could be lost to the force for action to be taken. The vans display appropriate signage and our public facing Privacy Notice covers the processing. As standard the asset should be added to the Asset Register, and the processing reason along with the DPIA documentation should be added to the force RoPA and reviewed at least annually or if a significant breach occurs.		
DPO advice accepted or overruled by:	Accepted by ACO Paul Bullen, Deputy SIRO	If overruled, you must explain your reasons
Comments: In coming to this view, I have considered the DPO advice. I have considered the lawful reason for processing this data (prevention and detection of crime) and the fact that this is a not a novel reason to process data i.e. speed camera enforcement is long embedded.		

There is a legitimate law enforcement reason to capture this data, and whilst there is a risk of data captured being lost through the manual process to take information from the systems on the vehicles, this is considered low (with a limited data set) and there is no history of breach. The broader data capture is subject to automatic weeding and therefore the removal of the data is swift. Signage is displayed to the public with regards the CCTV operation. Given all of this, I am content with the DPO advice. Should anything change within the DPIA then this should be referred back to the SIRO for further consideration.		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	M O'Connell Safer Roads Manager	The DPO should also review ongoing compliance with DPIA