SURVEILLANCE CAMERA COMMISSIONER

# Self Assessment Tool

## How well does your organisation comply with the 12 guiding principles of the Surveillance Camera Code of Practice? Complete this easy to use self assessment tool to find out if you do.

### Using this tool

This self assessment tool has been prepared by the Surveillance Camera Commissioner (SCC) to help you and your organisation identify if you're complying with the Surveillance Camera Code of Practice (the Code). It should be completed in conjunction with the Code, and can help to show you how well you comply with each of its 12 guiding principles.

It is possible to be largely compliant with some principles and to fall short against others. As a result you will note that at the end of the questions against each principle there is a space to include an action plan. This is so you can put actions in place over the next year to improve your compliance to that principle. These boxes can also be used to make a note of what evidence you could produce if required to show your compliance to that principle.

The template contains a combination of open and closed questions. For the open questions, there is a limit on how much you can write within the template, so please feel free to include any additional notes as an annex to the document – there are additional blank pages at the end of the tool to help you to do so.

Remember that your organisation may operate more than one surveillance camera system, with a scope that extends across several purposes and many geographical locations. So, before you start clarify the scope of the system(s) you propose to self assess for compliance against the Code.

### Is this tool for me?

The self assessment tool is aimed primarily at relevant authorities under Section 33 of the Protection of Freedoms Act 2012 who have a statutory duty to have regard to the guidance in the Code. In general terms, this means local authorities and the police in England and Wales.

If you work within any other organisation that operates surveillance camera systems you are free to adopt and follow the principles of the Code on a voluntary basis. If you decide to do so, then using this tool will be of benefit to you.

As a relevant authority under Section 33, if you are considering the deployment of a new surveillance camera system, or considering extending the purposes for which you use an existing system, you may find the more detailed three stage passport to compliance tool a valuable planning tool. It can guide you through the relevant principles within the Code and inform you of the necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the Code.

If you are from any other organisation operating a surveillance camera system you may find this template useful in reviewing your use of surveillance, or may want to use other SCC online tools such as the Data Protection Impact Assessment guidance or the Buyers Toolkit to help decide whether your surveillance is necessary, lawful and effective.

## What should I do next?

The self assessment is for you to satisfy yourself and the subjects of your surveillance that you meet the 12 principles and to identify any additional work necessary to show compliance. Think about realistic timescales for completion of your action plans, with a view to achieving full compliance with the Code before undertaking your next annual review.

The SCC does not want you to submit your completed self assessment response to him. However, in the interest of transparency he encourages you to publish the completed self assessment tool template on your website.

A completed self assessment is also a positive step towards third party certification against the Code.

Email the SCC at scc@sccommissioner.gov.uk to let us know when you have completed this template as this will enable us to understand the level of uptake. We would also appreciate your comments and feedback on the user experience with this template. Please let us know if you are interested in working towards third party certification against the Code in the near future, or would like to be added to our mailing list.

| | |
|---|---|
| Name of organisation | Leicestershire Police |
| Scope of surveillance camera system | Visual Recording Equipment |
| Senior Responsible Officer | Kerry Smith |
| Position within organisation | T/ACC and Force SIRO |
| Signature | |
| Date of sign off | August 2022 |

## Principle 1

Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

1. What is the problem you face and have you defined a purpose in trying to solve it? Have you set objectives in a written statement of need?

| |
|---|
| As part of the Authorised Professional Practice (APP) set by the College of Policing, it is highly desirable in pursuit vehicles to be fitted with visual recording equipment, for evidential purposes. As part of the APP it is required that the equipment is properly maintained and if not working to be reported at the earliest opportunity. Therefore officers from departments who routinely use Tactical Pursuit and Containment (TPAC) tactics have vehicles fitted with visual recording equipment. This includes vehicles from the Road Policing Unit and the Armed Response Vehicles, which consists of more than twenty vehicles fitted with these systems.<br>The Visual Recording Equipment (VRE) is in both marked and unmarked vehicles on these units. The object of the VRE is to obtain evidence as it it happens for a policing purpose, this is best practice and shows the incident as the officer witnesses it.<br>The APP provides the guidelines for forces and the Force Policy is currently being reviewed arround in car CCTV.<br>The footage can also be used for officer learning and development post incident where lessons can be mearnt .It could also be used by the IOPC and Professional Standards department should there be an officer complaint.<br>The Primary use is for Evidential Purposes and the secondary for Complaints/misconduct against Police officers/staff. |

2. What is the lawful basis for your use of surveillance?

| |
|---|
| Common Law<br><br>Police Act 1996<br><br>Road Traffic Act 1988 |

3. What is your justification for surveillance being necessary and proportionate?

| |
|---|
| Justified under its use in capturing evidence. Predominantly during police pursuits. Evidence that is gathered is downloaded to a standalone computer system and recorded as a Master Copy. A working copy is then produced on disc for evidential use. Any unrequired footage is overwritten similarly to standalone CCTV recordings.<br>The use of VRE is necessary due to the type of incidents attended by the Police, it is necessay to capture the the footage which will be required evidentially, the only other way the footage caught be good would be on the officers BWV but this would not have the same quality and would not pick up the front and rear of the police vehicle, it would also not pick up the speed of the potential pursuit.<br>The VRE is proportionate as this is only currently uitlised by Armed Cars, traffic and the |

area response car. The process for evidencing the footage has changed slightly since the implementation of the NICE Investigate System – we now have the ability to record an MP4 file of the footage on the stand alone computer – this is then exhibited on the NICE investigate system which has negated the need to produce a 'Master DVD' and a 'Working Copy' and allows the footage to be more easily shared with our CPS Colleges for both charging decisions and court viewing. The exception to this is where pre-emptive Tactics have been used but no 'crime' or other NICHE Report is created (A NICHE Record is required to upload evidence onto NICE) in this case the footage from the most appropriate vehicle (usually the rear car) is downloaded and stored on the 'H' Drive for pursuit / tactic review purposes.
Evidential Footage – any footage that is deemed to be evidential or has a NICHE occurrence number will be stored on NICE Investigate a hard copy is not produced and booked as the digital storage on NICE is sufficient
In case an incident happens in front of the vehicle spontaneously and there is no justification for retention , the recording is removed under force policy to prevent excessive processing.

4. Is the system being used for any other purpose other than those specified? If so please explain. ☒ Yes ☐ No

In significant court cases, with a pressing need, the Crown Prosecution Service has requested for the routes taken by defendants or victims of public places. This is completed by drive throughs of the route and is provided to court.
The footage can be used for disciplinary and misconduct matters by the IOPC or PSD.
The footage can also be used for learning and development.

5. Have you identified any areas where action is required to conform more fully with the requirements of Principle 1?

**Action Plan**

21/04/22
Confirm how long data is stored on the vehicle hard drive - A. The footage is stored on the hard drive until the drive is full and then the oldest footage is overwritten – the length of time this will take will depend on how much the vehicle is used but is generally around 3 / 4 weeks.
Confirm what measures are put in place when vehicles are sent out of force for repair to safeguard the data held within the vehicle A - To download the data you either need the correct computer program to access the hard drive by way of the Ethernet cable link or a key to remove the hard drive from the vehicle. The Key to the hard drive is not kept with the vehicle keys.
Confirm the process of training RPU/ARV officers for use of the download A-– the process of downloading the in car video is part of the RPU Officers input whilst with their mentor. There is also a step by step guide next to the download computer for ease of access.
Clarity on the access on NICE to the footage and any guidance circulated A-– All SSD RPU Officers have had e-mail advice to add any in car footage downloaded to NICE investigate where there is a NICHE number generated – IE FTS or some form of Crime / Incident recorded. Access to the footage on NICE is auditable but not restricted as a matter of course.
What non SSD vehicles have video facility and what measures are in place to ensure user compliance A- – LPD have a number of Vauxhall Insigna vehicles which were fitted with in car video

recording capability. There are a number of these vehicle still in use on NPA's. I am not sighted on what training or guidance was circulated in relation to the use of these vehicles – PC Adam Rowlands was part of the commissioning team – I have e-mailed him to ask if he has any details.

What facility is in place to report faults , and track progress A- – in relation to the download computer or download ports fault are reported to IT Faults and a IT Job number generated and tracked via Sunrise. Vehicle camera faults are reported to TU and logged on their recording system.

## Principle 2

The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

1. Has your organisation paid a registration fee to the Information Commissioner's Office and informed them of the appointment of a Data Protection Officer (DPO) who reports to the highest management level within the organisation?

☐ Yes ☐ No

2. Are you able to document that any use of automatic facial recognition software or any other biometric characteristic recognition systems is necessary and proportionate in meeting your stated purpose?

☐ Yes ☒ No

3. Have you carried out a data protection impact assessment, and were you and your DPO able to sign off that privacy risks had been mitigated adequately?

☐ Yes ☒ No

Before May 2018 the requirement was to complete a privacy impact assessment; this has been replaced by a data protection impact assessment. There is a surveillance camera specific template on the Surveillance Camera Commissioner's website:
https://www.gov.uk/government/publications/privacy-impact-assessments-for-surveillance-cameras

4. Do you update your data protection impact assessment regularly and whenever fundamental changes are made to your system?

☐ Yes ☒ No

5. How have you documented any decision that a data protection impact assessment is not necessary for your surveillance activities together with the supporting rationale?

DPIA required and in progress

6. Have you identified any areas where action is required to conform more fully with the requirements of Principle 2?

☐ Yes ☒ No

**Action Plan**

21/04/22

Q2 Principle 2 - N/A
Q3 -- The DPIA is in progress but has not yet been signed off therefore the risks have not been considered by the Data Protection Officer and signed off by the Senior Information Risk Owner.
Q4 DPIA is in progress and once it is signed off along with the measures. The Business Owner must ensure these are implemented and also ensure the DPIA is reviewed on a regular basis or when there is a change in process.

## Principle 3

There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

7. Has there been proportionate consultation and engagement with the public and partners to assess whether there is a legitimate aim and a pressing need for the system? ☐ Yes ☒ No

8. Does your Privacy Notice signage highlight the use of a surveillance camera system and the purpose for which it captures images? ☒ Yes ☐ No

9. Does your signage state who operates the system and include a point of contact for further information? ☐ Yes ☒ No

10. If your surveillance camera systems use body worn cameras, do you inform those present that images and sound are being recorded whenever such a camera is activated? ☒ Yes ☐ No

11. What are your procedures for handling any concerns or complaints?

The Force website specifies several ways how the police can be contacted about a variety of matters including the complaints procedure.- If a compliant is received by the system operator there are the policies and procedure relating to handling of complaints in general and the actions they should take. This would be cover a complaint with regards in car CCTV in the same way as any other formal complaint.

12. Have you identified any areas where action is required to conform more fully with the requirements of Principle 3? ☒ Yes ☐ No

**Action Plan**

21/4/22
Point 8 - Confirmation with regards privacy notice signage
Point 9 - Is in the process of being updated, with regard to all marked vehicles fitted with CCTV and ANPR having stickers indicate their presence. This is being worked on by Repographics and Vehicle Fleet. Chased for response 28/06/22 > TU Phillipa Spooner requested to ensure all marked cars are compliant when in for routine work
Point 7 -reasonable expectation from the public that the police will use CCTV in vehicles to obtain evidence for a policing purpose and will only be processed for that purpose. Sgt Steve Lewin asked to ensure officers are reminded of need to inform members of the public that they are being recorded .

## Principle 4

There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

13. What governance arrangements are in place?

Video footage is downloaded to a master standalone system, only accessed for the purposes of downloading footage. There are;

- o Clear policies and procedures in use (currently being updated)
- o Clear RRD procedures
- o Overt Surveillance Governance Board
- o Training

- Data Protection Impact Assessment is in progress

14. Do your governance arrangements include a senior responsible officer? ☒ Yes ☐ No

15. Have you appointed a single point of contact within your governance arrangements, and what steps have you taken to publicise the role and contact details? ☐ Yes ☒ No

Guidance on single point of contact: https://www.gov.uk/government/publications/introducing-a-single-point-of-contact-guidance-for-local-authorities/introducing-a-single-point-of-contact

There is a BWV and in car CCTV business lead who acts as the SPOC around Governance.

16. Are all staff aware of the roles and responsibilities relating to the surveillance camera system, including their own? ☒ Yes ☐ No

17. How do you ensure the lines of responsibility are always followed?

Only those individuals utilising the vehicles containing the VRE are responsible for using this footage.
In car CCTV policy and procedure has been written and circulated .

18. If the surveillance camera system is jointly owned or jointly operated, is it clear what each partner organisation is responsible for and what the individual obligations are? ☐ Yes ☒ No

19. Have you identified any areas where action is required to conform more fully with the requirements of Principle 4? ☒ Yes ☐ No

**Action Plan**

21/4/22
Point 14 - Confirmation as to who the senior responsible officer is
Point 15 - Confirmation as to who the SPOC is for governance
Point 16 - How sure are we that staff are aware of their roles and responsibilities A- Staff are given guidance when they join the RPU – they should all know to download footage that is evidentially required or is required for pursuit / tactics debrief purposes.
point 17 - In car CCTV policy and procedure is listed as under review - has this been signed off yet ?

## Principle 5

Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

20. Do you have clear policies and procedures in place to support the lawful operation of your surveillance camera system? If so, please specify.

☒ Yes ☐ No

21. Are the rules, policies and procedures part of an induction process for all staff?

☒ Yes ☐ No

22. How do you ensure continued competence of system users especially relating to relevant operational, technical, privacy considerations, policies and procedures?

Use of the VRE is limited to a small number of staff who utilise the vehicles, Line managers are responsible for Dip sampling the footage. Training is provided by the relevant department and with any officer new to the Department. No refresher trainning is provided, however a "how to" guide is provided with the computer and any updates are cascaded out to Officers.

23. Have you considered occupational standards relevant to the role of the system users, such as National Occupational Standard for CCTV operations or other similar?

☐ Yes ☒ No

24. If so, how many of your system users have undertaken any occupational standards to date?

N/A

25. Do you and your system users require Security Industry Authority (SIA) licences?

☐ Yes ☒ No

26. If your system users do not need an SIA licence, how do you ensure they have the necessary skills and knowledge to use or manage the surveillance system?

Specialist/advanced users only - Training, policies and procedures.

27. If you deploy body worn cameras, what are your written instructions as to when it is appropriate to activate BWV recording and when not?

N/A

28. If you deploy surveillance cameras using drones, have you obtained either Standard Permission or Non-Standard Permission from the Civil Aviation Authority and what is your CAA SUA Operator ID Number?

☐ Yes ☐ No

N/A

29. Have you identified any areas where action is required to conform more fully with the requirements of Principle 5?

☐ Yes ☒ No

**Action Plan**

21/4/22
Q 20 - Policy under review and once reviewed it will be on the Force Intranet - Policies.Has this been completed yet , if not what is the anticipated sign off date
Q21 - If rules and policies are part of an induction process where is this held to confirm compliance A-– In Car CCTV downloading is part of the RPU Officers PAC and will only be signed off once deemed competent by a current member of the RPU. The PAC is retained currently by the shift Sgt.
Q22 - Line managers dip sample - how often and where and how is this dip sampling recorded.No refresher training is provided , how do we evidence continued professional development and competence ?

Any requests for CCTV / In car footage need to be made via the current channels – IE Through Collision support for RTC's, at the request of PSD or as part of the investigation

## Principle 6

No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

30. How long is the period for which you routinely retain images and information, and please explain why this period is proportionate to the purpose for which they were captured?

Normal retention period for non Evidential is 30 day, in order for a crime to be recorded or complaint received. Downloaded data is retained for evidential purposes.
The APP on MoPI provides the following specific guidance in relation to the retention of evidential material, "There is a subset of policing information and records that relates to evidential material. This refers to any physical property, digital data or media that is downloaded or recovered, could form part of the evidence of a criminal offence and may become a court exhibit in any judicial proceedings. This could include downloads from mobile phones, bodyworn video footage and CCTV. This definition applies to both digital and physical evidence. Any unused evidential material should be examined as part of a robust post-case review and consideration should be given to the need for retention or disposal under the Criminal Procedure and Investigations Act (CPIA) 1996. Other evidential material should be retained in line with this APP. However, forces should work towards systems and processes that will allow the efficient deletion of evidential material within the CPIA 1996 timescales, in line with the National Police Chiefs' Council (NPCC) advice (currently under development - this has now been approved 'NPCC Management of Physical and Digital Evidence - National Retention and Review Guidance

– 3rd attachment). Metadata relating to digital material should be retained under MoPI as part of the record."

Retention periods as per the NPCC National Guidance on the minimum standards for the Retention and Disposal of Police Records;

- Bodycam / Headcam/Webcam - Non-Evidential - 30 days/Crime - Minimum of 6 Years, retain Case / Crime in accordance with MoPI/CPIA

- CCTV - Closed Circuit Television Tapes/Video tapes produced by any CCTV system used by a force e.g. custody - 31 days or relevant parts copied and retained as per MoPI rules or if the whole tape is evidential retain as per MoPI

- CCTV - Closed Circuit Television Tapes. Video tapes not owned by a force but needed for evidential purposes - Minimum of 6 years / review as per nominal file in accordance with MoPI/CPIA

31. What arrangements are in place for the automated deletion of images?

The in car system has a finite amount of space on the Hard Drive – once this is full the footage auto overwrites the oldest footage – this will depend on how often the vehicle is used as the system will not record when the car has been stopped and the ignition turned off for longer than 10minutes. It may be possible to set up the system to auto delete the in car footage after a set period of time as opposed to it being the oldest footage to be overwritten. Usually there is enough storage space on the hard drive to record 2 /3 weeks' worth of 'usual' use. In relation to the stand alone computer – the files currently do not have an auto delete option – the stand alone computer only has footage that has been

downloaded for evidential purposes IE Speeding offences, Road Traffic Offences, Pursuits or pre-emptive tactics etc. This may be an issue that would need looking into to comply with Data Protection Act 2018.

32. When it is necessary to retain images for longer than your routine retention period, are those images then subject to regular review? ☒ Yes ☐ No

33. Are there any time constraints in the event of a law enforcement agency not taking advantage of the opportunity to view the retained images? ☒ Yes ☐ No

34. Do you quarantine all relevant information and images relating to a reported incident until such time as the incident is resolved and/or all the information and images have been passed on to the enforcement agencies? ☒ Yes ☐ No

35. Have you identified any areas where action is required to conform more fully with the requirements of Principle 6? ☐ Yes ☒ No

**Action Plan**

21/4/22

Q31 -Auto delete option to be explored and confirmation that current system os use is compliant A- – I am not aware that any auto delete is currently installed on the download computer to delete non saved footage. The in car hard drive overwrites its self once full – dependant on the amount of use of the vehicle the time for this currently varies.
Q32 - What is the current process for review of images A - – in car video can currently be reviewed either by connecting the vehicle to an external Ethernet port and then using the specific download software on the stand alone computer – the footage is either then held on the hard drive or uploaded to NICE Investigate. Best practice would be for any footage that is linked to a NICHE Occurrence is to be uploaded to NICE Investigate which is a auditable system. The footage held on the stand alone hard drive can be accessed by anyone who knows the password – the folders are not password protected and there is a single sign on to the computer so no audit trail.

## Principle 7

Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

36. How do you decide who has access to the images and information retained by your surveillance camera system?

This is role based and access is provided to officers who are Initial Pursuit or TPAC trained utilising in-car video as per the APP.

37. Do you have a written policy on the disclosure of information to any third party? ☒ Yes ☐ No

38. How do your procedures for disclosure of information guard against cyber security risks?

'The Force IT Infrastructure is secured in-line with national policing requirements, with an annual assessment conducted by the Police Digital Service, to assure this, with this process supplemented by an annual penetration test of our environment, alongside internal processes such as the use of vulnerability management software to routinely scan our environment and remediate any vulnerabilities identified. The Force also benefits from the protections afforded by Office 365 utilising a number of these tools to safeguard our environment, with safeguards in place to safeguard our on-premise environment such as perimeter safeguards, encryption, anti-virus/anti-malware tools etc. The Force have a close working relation with the National Management Centre, who provide a number of services to Forces – protective monitoring, cyber threat intelligence and remediation advice etc.

Robust security incident management processes are in place within the Force and documented within bespoke procedures (both Cyber and traditional security incidents). An escalation process is in place to ensure that notification occurs to the relevant stakeholders within a timely manner, and within the legislated timeframe.

39. What are your procedures for Subject Access Requests where a data subject asks for copies of any images in which they appear?

SARs are processed through the Forces Information Management Dept. The is a currently procedure Subject Access and Disclosure on the internal page.

40. Do your procedures include publication of information about how to make a Subject Access Request, and include privacy masking capability in the event that any third party is recognisable in the images which are released to your data subject? ☒ Yes ☐ No

41. What procedures do you have to document decisions about the sharing of information with a third party and what checks do you have in place to ensure that the disclosure policy is followed?

| |
|---|
| VRE from in-car video has been provided to the Crown Prosecution Service and only contains evidential material, this release of information is signed of by a line manager and case buider in the form of a file of evidence. Should any additional requests arise other than the CPS then this will be refered to and dealt with under the direction of the information management department . |

42. Have you identified any areas where action is required to conform more fully with the requirements of Principle 7? ☒ Yes ☐ No

**Action Plan**

| |
|---|
| 21/4/22<br>Q36 - Is there a difinitive list of all officers authorised to access the info and images A- – Not a specific list however it would be anyone currently working on the RPU and ARV Teams<br>Q37 - Confirmation that the written policy exists and where can it be located |

## Principle 8

Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

(There are lists of relevant standards on the Surveillance Camera Commissioner's website: https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry)

43. What approved operational, technical and competency standards relevant to a surveillance system and its purpose does your system meet?

Standards are set by the required purpose of the equipment. This has been set by the Authorised Professional Practice (APP) from the College of Policing.Suppliers must conform with BS EN( British and European Standard )

Upon a vehicles return to headquarters post patrol, all data is uploaded to a non-networked terminal, which has undergone appropriate hardening in line with the guidance published by the NCSC. Upon ingestion, all data undergoes anti-virus/anti-malware scans. Should the data be identified as "evidential", the data is transferred to a secured network. This network undergoes an annual assessment, including penetration test and subsequent remedial actions of identified vulnerabilities, to ensure that it meets the UK policing standard, PSN for Policing. The assessment of the network is completed by the National Police Information Risk Management Team (NPIRMT).

Upon the data being transferred to the secured network, the data is uploaded to select for systems, for processing. These systems have undergone a robust assurance process to ensure their suitability for use within a policing environment. Access is governed by the "least privilege" principle/"need to know basis". Audit trails are maintained for every action undertaken by Force users, with any suspected misuse referred to the Professional Standards Department for review, and a security incident report raised.

44. How do you ensure that these standards are met from the moment of commissioning your system and maintained appropriately?

A review panel consisting of Supervisory and super users has considered the most appropriate equipment to be used, to ensure it meets operational, technical and competency standards.This happens on an adhoc basis, this is only in relation to the equipment and not the storage.

45. Have you gained independent third-party certification against the approved standards? ☐ Yes ☒ No

46. Have you identified any areas where action is required to conform more fully with the requirements of Principle 8? ☒ Yes ☐ No

**Action Plan**

The system(s) used currently are not fit for purpose – they are unreliable and you can buy a base model dash cam which provides better quality images than the cameras we currently use. The download system is also far behind the times – having to physically connect the vehicle to a download computer is antiquated, also having to use a separate stand alone download computer is a barrier to footage being downloaded when needed, we also have issues with handling of footage and retention times. Insp 1076 is scoping alternative systems which will require a business case for purchase,

Q45 - If we have not had any independent certification against standards what system is in place for us to sense check what we do and how we do it in relation to compliance ?

## Principle 9

Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

47. What security safeguards exist to ensure the integrity of images and information?

Hardrives within the vehicles are secured and locked in place. The devices are encrypted and can only be downloaded with the appropriate equipment. The standalone system is contained within the secure Headquarters site and a secure building. ( the access to the building is controlled and auditable )

This standalone system is password protected. As such, only users requiring it to dowload the system can access it.

It would also depend on where the data is stored – the stand alone computer has a single user sign on with a password, as such is it not possible to see what each officer has been viewing on the Stand Alone Computer. Footage stored on NICE will have an audit trail of who had access (contained within the NICE Investigate system) however there is no pro active checking or monitoring of whom has accessed the footage from an RPU perspective.

In relation to any back-up – I am not aware of the stand alone computer being backed up however any evidential footage should be stored on the NICE Investigate System.

48. If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist? ☐ Yes ☒ No

49. How do your security systems guard against cyber security threats?

Not conntected to network. Standalone system.

50. What documented procedures, instructions and/or guidelines are in place regarding the storage, use and access of surveillance camera system images and information?

Instructions for download are provided with system - RSG Website and with NICE investigate Officers have been trained around the use of transferring data.

51. In the event of a drone mounted camera being lost from sight, what capability does the pilot have to reformat the memory storage or protect against cyber attack by remote activation?

N/A

52. In the event of a body worn camera being lost or stolen, what capability exists to ensure data cannot be viewed or exported by unauthorised persons?

| |
|---|
| N/A |

53. In reviewing your responses to Principle 9, have you identified any areas where action is required to conform more fully with the requirements? If so, please list them below. ☒ Yes ☐ No

**Action Plan**

| |
|---|
| 21/4/22<br>Q47 - Currently there is a single sign on to the stand alone computer and we cannot know who has accessed the system - requires review A- – currently the way the software licence works means we can only have one ‘user’ as such we only have the single sign onto the computer. The computer is also not a networked computer so it would be technologically difficult to create all the users that we require for individual sign on.<br>There is also no back up for this stand alone system - can this be correct? A-any evidential footage should not be stored on there and should be on NICE Investigate. |

## Principle 10

There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

54. How do you review your system to ensure it remains necessary and proportionate in meeting its stated purpose?

APP requiring Visual Recording Equipment. Officers who use the device review the use of the system and have highlighted an element of risk around it not being connected to the force system. The regular review of the DPIA will assist in the system remaining necessary and proportionate.

55. Have you identified any camera locations or integrated surveillance technologies that do not remain justified in meeting the stated purpose(s)? ☐ Yes ☒ No

56. Have you conducted an evaluation in order to compare alternative interventions to surveillance cameras? (If so please provide brief details) ☐ Yes ☒ No

57. How do your system maintenance arrangements ensure that it remains effective in meeting its stated purpose?

All six Roads Policing Sgts and Inspector oversee the management of the Visual Recording Evidence system. Any faults identified are brought to the attention of the transport unit , or the organisations IT department via the faults helpline .

58. Have you identified any areas where action is required to conform more fully with the requirements of Principle 10? ☒ Yes ☐ No

**Action Plan**

21/4/22
Q57 - Who are the staff tasked with overseeing management and maintenance ? A- Maintenance is overseen by the transport uni who book the contractor staff to come in to look at any issues.

Monitor and audit mechanism requires review

## Principle 11

When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

59. Are the images and information produced by your system of a suitable quality to meet requirements for use as evidence? ☒ Yes ☐ No

60. During the production of the operational requirement for your system, what stakeholder engagement was carried out or guidance followed to ensure exported data would meet the quality requirements for evidential purposes?

Consultation took place with the Crown Prosecution Service (CPS) to make sure the footage was of an acceptable evidence quality.

61. Do you have safeguards in place to ensure the forensic integrity of the images and information, including a complete audit trail? ☒ Yes ☐ No

62. Is the information in a format that is easily exportable? ☒ Yes ☐ No

63. Does the storage ensure the integrity and quality of the original recording and of the meta-data? ☒ Yes ☐ No

64. Have you identified any areas where action is required to conform more fully with the requirements of Principle 11? ☐ Yes ☒ No

**Action Plan**

- System needs to be put in place to ensure image quality is monitored
- Requirement for a regular maintenance programme for the system needs exploring
- Information required as to how many times the SD card can be written over

## Principle 12

Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

65. What use do you make of integrated surveillance technology such as automatic number plate recognition or automatic facial recognition software?

N/A.

66. How do you decide when and whether a vehicle or individual should be included in a reference database?

N/A

67. Do you have a policy in place to ensure that the information contained on your database is accurate and up to date? ☒ Yes ☐ No

68. What policies are in place to determine how long information remains in the reference database?

N/A

69. Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000? ☒ Yes ☐ No

70. Have you identified any areas where action is required to conform more fully with the requirements of Principle 12? ☐ Yes ☒ No

**Action Plan**

- Confirm RIPA is included in the induction for new officers / users