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	Police SUAS (Drones)
Senior Responsible Officer	Kerry Smith
Position within organisation	T/ACC and Senior Information Risk Owner
Signature	
Date of sign off	Aug 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?

Leicestershire Police currently utilise drones in order to deliver policing more effectively. Drones are used for Pre-Planned Events such as Sporting Events, Festivals and Protests to assist with crowd monitoring and to respond to incidents at these events quickly and effectively. Drone are also deployed to spontaneous Incidents such as missing and vulnerable person searches, searching for offenders and assisting other emergency services during major incidents, using the JESIP Principles. Drones allow the Police to search and monitor large areas quickly, by utilising increased sight lines from the Drone at altitudes up to 400ft. Drones can also be used by Leicestershire Police to approach incidents safely, by placing a drone into the incident location as opposed to people. Such an example of this is when assisting Leicestershire Fire and Rescue Service at multi-agency fire and rescue incidents.

Drones are always used in pursuit of meeting a Policing Purposes, defined as

1. Protecting life and Property
2. Preserving Order
3. Preventing the commission of offences.
4. Bringing offenders to justice
5. Any duty or responsibility of the Police arising from common law or statute.

Leicestershire Police will always deploy in-line with the approved operations manual.

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

The Human Rights Act 1998 Article 2 (Right To Life), Article 5 (Right To Liberty), Article 6 (Right To A Fair Trial), Article 8 (Right To Private Life), Article 10/11 (Freedom Of Expression And Assembly).

Crime And Disorder Act 1998 - Implementing Strategies To Help With The Reduction Of Crime and Disorder In Our Communities.

Regulation of Investigatory Powers Act 2000, MOPI, CPIA, GDPR, DPA, SCC COP and Common Law are applicable.

Common Law - Duty of a constable

Police Act 1996

Any additional legislation identified as applicable to the purpose of the use of the drone, identified at the popint of deployment.

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

Justified under the HRA as necessary and proportionate and in the interests of national security, public safety, the prevention and detection of crime and the protection of health. It is used to help detect, deter and disrupt criminality at local, force wide and regional levels. Drones are also deployed for matters involving public safety. Drone Pilots are provided with specific training, during their initial pilot training, with regards to surveillance camera commissioner principles and will deploy Drones in a manner that minimises impact on the privacy of individuals. Refresher training will be provided during yearly CPD. Drones are a far more cost effective Tactical Option, causing less disturbance to the public when compared to the National Police Air Service (NPAS).

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

No

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

Action Plan

None identified

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?

N/A - DPIA has been completed, reviewed 04/06/2022.

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

☐ Yes ☒ No

Action Plan

Notes

2. Leicestershire Police Drones Do Not Utilise Facial Recognition Software At This Time.

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?

Leicestershire Police Website specifies several ways how the police can be contacted about a variety of matters, including the complaints procedure. If complaints are made against officers, our Professional Standards Department will handle this and if required are passed onto the IOPC (Independent Office For Police Conduct).

Members of the public who have privacy related concerns or complaints are able to contact our Information Management department. Information Management are the central point of contact for both privacy and subject rights issues. Any complaints with regards to privacy will be referred to the ICO by the force.

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

Action Plan

Additional Information

7. The use of Drones has been advertised by Leicestershire Police and the reasons for its use explained, this is completed by way of Facebook and Twitter.

8. Current Signage is deployed at the drone Take-Off and Landing Position. The sign informs members of public of the use of drones, however it does not state the purpose for which it captures images, as this purpose would change dependent on the taskings taking place, therefore it is impracticle to have a sign large enough to state all the possible purposes. Officers will be within sight of the signage and are happy to be approached and asked about the Drone.

9. Signage is used which states 'Police Drones in Operation' when drones are deployed. Signage does not state who is the point of contact, however Officers will be within sight of

the signage & Drones.

10. Drones do not use Body Worn Cameras, but the officers who deploy the drones do carry Body Worn Cameras. Body Worn Cameras are always utilised during deployments to record the initial launch of the Drone, in order to record the fact the Safety Checklist has been followed.

Action Plan

12. Consider the creation a fact sheet to be handed to members of the public who ask for information about drones / privacy concerns.

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?

All Officers within force are vetted. Officers who operate Drones for Leicestershire Police do so under the approval and authorisation of the Accountable Manager and only once they have completed the required CAA Training Course. Following the completion of a CAA Training course, additional internal training and assessments are conducted. This internal training covers data protection and information management, but additionally provides guidance as to when images are to be captured with a drone. Images are not captured during every flight as recordings are only made when the drone is on-task at the discretion of the Pilot (I.E the drones are not set up to 'always record'), for example with a drone not recording imagery during transit to a task. All recordings will cease as soon as the objective of the flight has been met.

Access to the Drones is restricted, through the Drones being housed in a lockable storage area, where only trained pilots have access. The storage area is located within a building with controlled access, only authorised to those that require to do so, as authorised by their line-manager.

In terms of the images captured by the Drone, Evidential Footage is transferred to a Secure Case File System within Leicestershire Police's Corporate Memory. Access to the system is monitored and auditable, with the Officer in the case restricting access if the nature of the imagery is sensitive. In terms of Non-Evidential Images, these are transferred to an Imagery Folder and either labelled with a Weed Date Of 28 days and then manually deleted or for images captured that only hold Police Footage and are required for either internal Training or Public Consultations/Presentations, these are labelled as such and retained in the imagery folder. This retained footage will not contain images where persons are indetifiable and will be subject to redaction if required to ensure the privacy of members of the public is maintained. This Imagery Folder has restricted access and can only be viewed by Authorised Staff on the Drone Team. Access to the folder will be revoked if staff cease to be involved in the capability.

In terms of the Secure Case File System, when the Data is extracted by the User/Officer In The Case that system has a reminder for all users of their responsibility in terms of the Data Protection and the Retention Policies. Data will generally only be extracted when it is produced as evidence for court.

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

The Single Point Of Contact is Ch Insp GILLARD who is the Drone Teams Accountable Manager, this has been doumented in the Leicestershire Police Operations Manual and with the Civil Aviation Authority.

Leicestershire Police are also currently in the process of creating a drone page on the forces website, where members of the public will also be able to see the governance of the Drone Operations.

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?

Each pilot is made aware of their responsibilities and has access to a workflow chart which details what constitutes overt and covert use of drones and responsibiltiies around RIPA. All flights are auditable through a restricted database and a procedure exists where Drones have to be signed out and back in by the pilots.

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

15. Page on Leicestershire Police Internet Website is currently being worked on.

17. The Drone Team Operations Manager (Sergeant) to be briefed on this and a plan created with regards to implementing an oversight regime to ensure compliance.

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?

Leicestershire Police provides annual training to its Pilots. These training inputs cover procedures in practical use of Drones, but also the responsible recording and handling of data. Pilots are line checked yearly to ensure compliance with the operations manual and the privacy impact assessment, but can also be subject to an assessment at any time. Line checks ensure compliance with both internal standards, as laid out in the Operations Manual, but also the external standards, as set out by the CAA within the Air Navigation Order.

During yearly pilot line checks, pilots are reminded of their responsibilities in terms of data handling and that it is either evidential and is uploaded to the Secure Case File System or Non-Evidential and is uploaded to the restricted access imagery folder, with a weed date being assigned if the footage is not required for training purposes.

The Drone Pilots are aware of their responsibilities to review the imagery folder and delete footage when it reaches its weed date.

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?

All Police Drone Pilots are required to complete an RAE (Recongises assesment entity) course in order to achieve a standard to satisfy the CAA's requirements. Pilots are then subject to an internal training and assessment process prior to being deployed

operationally to ensure competance in the required skills and knowledge in order to manage to system.

This training and assessment process covers all necessary skills and knowledge around the use of Drones, but also how the data that is captured is subsequently handled.
Each Pilot has to maintain Pilot Flight Currency of 60 minutes per month and this is monitored by the Flight Safety Manager in order to ensure compliance.
Those Pilots not meeting this currency will be withdrawn from the role until a Line Check has been completed by the Flight Safety Manager or in instances where this relates to the Flight Safety Manager, look to another force will conduct the Line Check.

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

PDRA01 Operational Authorisation
CAA ID - 6393
Operator ID is obtained and renewed yearly.

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

☐ Yes ☒ No

Action Plan

None identified.

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?

Evidential data, or data identified as meeting a Policing Purpose is retained in line with force policies for retention of footage.
All other data is retained for 31 days and then deleted.
All data is retained on secure, password protected systems with controlled internal access only.

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

After each deployment the data on the Drone Hard Drive and/or SD card is either:

1) Transferred to a Secure Evidential Case File System which only authorised staff can view, this will ordinarily be staff involved in the investigation of crime or incident. This is subject to an auto-deletion process.

2) Transferred to A Secure Imagery Folder with restricted access to Drone Pilots and a Weed Date (28 Days) Assigned, this folder is reviewed on a regular basis and footage deleted when weed date reached. There is no automated deletion within this system, the responsible officer must delete it manually after the Weed date.

All evidential footage is retainedin accordance with ECHR Article 8.

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

Q31 - Work is underway to implement an auto-delete facility for non-evidential footage. Evidential footage will continue to be managed on the Digital Evidence Case File (DECF) system by the OIC, as retention of evidential footage is on a case by case basis.

An interim measure has been put in place so that non-evidential footage is assigned a weed date (in line with the retention policy) and then manually deleted by officers on that date.

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?

Force policy deals with accessing force systems for a policing purpose only, and systems are auditable to enforce this.

Non-evidential footage is only accessible to officers within the Drone Team who require it for either review or ongoing training.

Evidential footage is stored on the Digital Evidence Case File (DECF) system or NICE, with officers and staff who require access manually being added to this by a member of the Drone Team in order to ensure controlled, auditable, access to evidential materials is maintained.

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?

Data is usually only disclosed when it is either required evidentially or for a specific, lawful purpose, in line with current force policies.

All requests for disclosure of footage are addressed in liasion with the Privacy Officer and disclosures are completed in line with secure data handling procedures.

As stated all data is stored with restricted access and accessible by all members of staff, therefore Cyber Security Risks are negated.

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.

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?

The Force has a variety of Information Sharing Agreements with our partner agencies such as Local Councils. In such circumstances, specifically where Drone Footage is concerned, an agency can make a request for imagery held in relation to an operation or deployment. If the request is justified, proportionate, legal and necessary, a search of our Drone tasking database will be carried out to check if a deployment had been conducted during the specified time period. Any identified deployments will then be checked to see if footage was obtained. Imagery will then be reviewed to see if it is relevant to the request and following consultation with the Privacy Officer, the imagery will be released if it is deemed legal, necessary and proportionate. Footage, or sections of captured footage, specific to the request will only be released. If redaction of any areas of the footage is required this will also be completed.

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

Action Plan

None

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?

No national standards (as listed above), or specific national Policing standards currently exist for Drones. The Drones owned by Leicestershire Police have been chosen as they meet operational, technical and competency standards identified by the organisation.

The system for retaining data is currently under review in order to improve practices, however all data is securely stored with controlled access.

These standards are referenced within the Leicestershire Police Operations Manual.

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

Procurement procedures are followed to ensure the most appropriate equipment is aquired that meet the required operational, technical and competency standards. If equipment fails to meet these standards, it is recorded and addressed with the manufacturers and suppliers. The team continues to monitor the development of Drone technology to ensure that the standards are maintained.

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

None

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?

Extensive firewalls exist to safeguard the system and data held. All systems are password protected, with the robustness of passwords required in line with IT policies.

Only officers within the Drone Team have access to non-evidential images. Evidential images are held on a separate system where access is auditable and recorded.

Drones are never left with Data Stored on either the internal hard drive or SD Card, Pilots are aware of their responsibilities to download the data from the internal hard drive or SD card before ceasing duty.

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?

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. Police data cannot be stored on personal mobiles. Regular reminders to members of the Force not to open emails.

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

Code Of Practice On The Management Of Police Information (MOPI)

DPIA and the Operations Manual, document procedures in place.

Access to the systems is restricted to trained officers only, with the systems being securely stored in a restricted building, office & lockers - with only Drone Officers having access. Handling of data is document in the Privacy Impact Assessment.

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?

All drones have the ability to have memory cards remotely wiped when beyond line of site, as long as the Drone is still within radio transmission range.

Newer aircraft being introduced have encrypted internal SSD Hard drives which require a password to access, older Drones have SD cards only which are not encrypted.

All SD Cards are downloaded and formatted following deployments to mitigate risk.

In the event of loss of a Drone or Camera through an unexpected emergency with the Drone i.e a Crash or a Flyaway, emergency procedures are in place to track movement of the Drone and utilise both Drone and other Police Staff to recover the Drone. This is standard pratice for all Drone Emergency Procedures and are documented in the Leicestershire Police Operations Manual. Drones are always deployed with a minimum of two staff, allowing sufficent staff to manage any emergency incident.

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

47. Data handling practises to be formalised into Standard Operating Procedures.

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?

The Operations manual and Privacy Impact Assessment are subject to a yearly review as a minimum. Updates to these documents are completed if required sooner than the scheduled date (E.G changes in legislation which effect the documents).

Officers authorised to use Drones are subject to annual assessments to ensure compliance with the documents. This is documented in pilots training and assessment folders. Each flight is debriefed by the Pilot and Observer where identified issued can be raised, these can then be fed back to the Operations Manager, flight safety manager and the accountable manager for action.

Drone equipment and the related systems are subject to continual review and monitoring to ensure it meets the current purpose. Review of equipment is conducted on a yearly basis and discussed during the Drone Board meetings an a bi-monthly basis.

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

Not Applicable

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

A small core team of police officers oversee the management of the Drone equipment, therefore any faults are quickly reported, logged and minor repairs completed in house if possible. All Drones are subject to a process of duty start inspections, therefore any faults are recorded and documented. If a fault is detected that requires the aircraft to be defected, this will be clearly documented and reported to the Flight Safety Manager. If repairs are unable to be completed in house - the drones are sent to an approved external repair centre. A service agreement is in place so that replacement equipment is provided in the interim to maintain operational service levels. All Drones are maintained in line with the manufacturers recommendations.

Imagery stored within the force network are subject to force maintenance requirements and will….

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

Action Plan

N/A

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?

Engagements with all departments that utlise the Drones capabilities have taken place to ensure that both the Drone Equipment used and Footage Produced would be of evidential quality and therefore is able to be used for Evidential Purposes.

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

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?

None in relation to Drones at this time.

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

N/A