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.

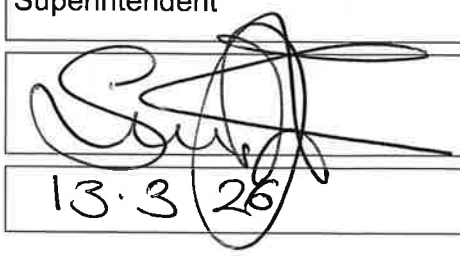
What should I do next?

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.gsi.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	West Midlands Police (WMP)
Scope of surveillance camera system	Overt use of Drones
Senior Responsible Officer	Simon Inglis
Position within organisation	Superintendent
Signature	
Date of sign off	13·3·26

SURVEILLANCE CAMERA COMMISSIONER

Self Assessment Tool

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?

West Midlands Police deploy drones in order to Prevent/Detect Crime and to Protect our Communities.

Drones are utilised on Pre-Planned, intelligence led operations such as Sporting Events, Protests, Festivals etc

They can also be deployed to spontaneous incidents, for example, searching for offenders or missing/vulnerable persons.

West Midlands Police work closely with partner agencies and deploy accordingly, using JESIP principles with other emergency services.

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

Crime and Disorder Act 1998 - Implementing strategies to help with the reduction of Crime and Disorder in our communities.

The Human Rights Act 1998 Article 2 (Right to Life), Article 5 (Right to Liberty), Article 8 (Right to Private Life), Article 10/11 (Freedom of Expression and Assembly), Article 6 (Right to a Fair Trial)

Data Protection Legislation (GDPR and the Data Protection Act 2018): WMP processes personal information in accordance with the Act, which exists to ensure the fair and lawful use of personal data and to protect the rights of the data subject.

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

Drones are used by WMP only in pursuit of a legitimate, and lawful aim. They effectively capture aerial imagery, helping to detect, deter, disrupt criminality and increase public safety.

Drones are a cost effective tactical option that work in harmony with the National Police Air Service (NPAS). Drones are less intrusive than other options and provide support with minimal impact to our communities.

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

Not Applicable.

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

Action Plan

No.

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?

Not Applicable.

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

☐ Yes ☒ No

Action Plan

In relation to question 2. West Midlands Police Operations Drones do not use automatic facial recognition software or biometric characteristic recognition sytems.

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?

West Midlands Police has a general complaints procedure and reporting system in place. This would be implemented and then refered to the Department of Professional Standards if required to do so and investigated in line with Force Policy.
All Drone related complaints are brought to the attention of the forces Accountable Manager. The Accountable Manager will investigate and deal with any outcomes, in collaboration with Professional Standards.
Professional Standards will be contacted annually to obtain information and data around the number and nature of complaints received and how they have been resolved. This will will be available for publication, if required.

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

Action Plan

In relation to question 10, this assessement is focused on Drone usage which does not form part of Body Worn Camera operation. A separate self-assessment has been completed for Body Worn Cameras which details their use.

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?

The force SRO chairs a bi-monthly Overt Surveillance Governance board which is minuted. The outputs from these meetings are fed into the Force Executive Team via the Operations ACC.

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

Inspector Mark Colwell is the Force's Accountable Manager in relation to Drones. This is publicised within our Operations Manual and with the Civil Aviation Authority.

To promote legitamacy/transparency we have also published a community information page detailing our Drone Use and this document on www.west-midlands.police.uk/frequently-asked-questions/police-drones.

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?

Every Pilot receives specific training in relation to what constitutes Overt/Covert Use of Drones and their responsibilities in relation to RIPA. They receive advice and guidance in the use of cameras, with an emphasis on recording only when necessary and for a legitimate policing purpose.

Staff have built a strong relationship with the Covert Authorites Bureau Specific and are able to seek advice and guidance where necessary. Incidents can also be discussed and guidance given through the Force Overt Surveillance Governance board.

WMP Operations, deploy uncrewed aircraft overtly and in compliance with the local Standard Operating Procedure and the Operations Manual which is submitted to the Civil Aviation Authority each year when applying to fly commercially. Pilots are tested frequently on their understanding of their responsibilities detailed within these documents, the law and the Police Code of Ethics.

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

In relation to question 18. Our surveillance camera system, the Drones, are not jointly owned/operated.

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?

Regular Continued Professional Development inputs covering areas such as RIPA are in place.
In addition, pilots are formally assessed at least once a year and tested on their knowledge and understanding of the surveillance principles.

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?

Not Applicable.

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 pilots are trained and accredited by a CAA approved provider and then complete a 5 day police drone input conducted by qualified police instructors which include detail around surveillance systems.
Each pilot is aware of the process used to authorise Drones for either a Pre-Planned or Spontaneous Incident. This is recorded within our Operations Manual.
All operators maintain a flight currency of 2 hours every 3 months and are monitored on this by the Flight Safety Manager(s).
Each pilot undergoes annual CPD incorporating theory and practical assessments.

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?

Not Applicable.

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

WMP Drones hold a CAA Operational Authorisation in the Specific category operating to a standard PDRA/01.

Operator ID:GBR-OP-M54YNLJN5RRM

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

☐ Yes ☒ No

Action Plan

Not Applicable.

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?

30 days - In line with the current force Evidence Gathering Policy

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

Drones internal storage/SD cards are regularly reformatted and any unused data is deleted.
All evidential footage is retained as per the evidence gathering guidelines and in accordance with ECHR Article 8, paying particular attention to Wood vs Metropolis (retention of images)

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

Evidential images/video/data are now transferred directly from the aircraft/sd card onto the Axon server via Evidence.Com.

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?

Only officers in the case, commanders and operators and officers who require access have access to evidence.com in line with current guidelines. Viewing of footage requires a officers log in and reason for viewing to be documented.
Evidential material is held on a secure server via: Evidence.com.

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?

Much like Body Worn Camera footage, evidential drone material is held on a secure server (AXON) which has been fully tested to ensure the risk of breaches are as low as reasonably possible.

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

If a subject requests footage the request will come via the Investigating officer or Officer in the case and in line with Force Policy.
Images held on the server can be released upon a reasonable request.
It's possible to blur / pixalate images recorded which do not have any relevance to the Subject Access Request.

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 WMP Internet Site provides our community with information relating to the holding of information, access rights and processes to follow in regard to access requests and/or FOI.

So long as there are no on-going investigations or proceedings anyone involved in a crime - victims, witnesses or offenders, can ask for their own data using the Subject Access provisions contained within the Data Protection Act.

This can be done by filling in form WA162 which is on the West Midlands Police website.

This process allows them to apply for their own personal information which may be held on West Midlands Police information systems.

WMP Information Management department manage and document requests made.

Information Sharing Agreements are in place which help govern the appropriate release of information with partners who we frequently share information with. They give our teams the confidence to release information critical to policing and safeguarding activity, but also the confidence to say no when it isn't justifiable.

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

Action Plan

Not Applicable

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?

There are no national standards at this time for the deployment of Drones.
That said, there are several pieces of national legislation that cover pilots and Drone usage placed in Commercial Operators (WMP is classed as a Commercial Operator). All of these are referenced within our Operations Manual, that is approved by the CAA on a annual basis.

The NPCC and the National Police Air Service are working together to introduce oversight of drone procurement, training and operational standards for policing and to develop Standard Operating Procedures and training materials, including compliance and safety management. WMP are actively supporting this work and will abide by the recommendations and guidance that is circulated.

NPCC guidance on the use of DJI technology dated 22nd February 2023 has been fully adopted by WMP.

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

Each Pilot has access to a copy of the Operations Manual and is informed whenever there are legislative changes made by the CAA.
Each pilot undergoes annual CPD where their knowledge of the Operations Manual and legislation is tested, both theoritcally and practically.

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

At the force governance board there will need to be a discussion and decision regarding the desire of the organisation to have this area of overt surveillance formally accredited via the third party certification scheme. If the decision is to seek such accreditation, further consultation will take place with the force executive team regarding funding for such activity.

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?

Drones operated by WMP are either password protected or can be remotely wiped to safeguard any data collected. At the conclusion of each deployment a decision is made to either delete or transfer the data securely to Evidence.Com, in line with MOPI (Management of Police Information) principles. Following transfer the SD card is reformatted. Footage is kept to an absolute minimum and is proportionate and legitimate.

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?

A detailed Data Protection Impact Assessment/Risk Assessment has been completed by a WMP Security Information Advisor providing assurance that procedures relating to the storage of drone footage are robust and compliant.

In addition to on-board drone data, WMP IT infastructure is tested frequently to prevent unwanted penetration and all new hardware/software is rigorously assessed prior to use.

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

Operational Standard Operating Procedures.
West Midlands Police Operations Manual
Code of Practice on the Management of Police Information (MOPI)
Surveillance Camera Code of Practice
Data Protection Impact Assessment - Drones

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?

The SD card and aircrafts on-board memory can be reformated via the ground station up to 4KM away at any point in the event of a "flyaway".
Aircraft internal memory is password protected where available.

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?

Not Applicable.

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

Not Applicable.

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?

Every operational Drone deployment is assessed to ensure that the deployment is necessary in line with the PLAN principles.
Operational deployments can be reviewed through governance arrangements.

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?

Drones are regularly serviced in line with manufactures' recommendations.
In addition, each Drone is visually inspected before and after every flight. Any damage noted and recorded and dealt with accordingly.
Each Drone is stored securely within a Police building with controlled access.
If Drones are sent to a third party for repair/service any stored images are deleted prior to being sent away.

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

Action Plan

Not Applicable.

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 Investigating officers and officers in charge of investigations to ensure what was capable of being produced had evidential sufficiency.

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

Not Applicable.

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?

At this time, Operations Drones do not make use of any of the aforementioned systems.

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

Not Applicable.

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?

Not relevant.

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

Not Applicable.