

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	Kent Police
Scope of surveillance camera system	Drones
Senior Responsible Officer	Chief Superintendent Amanda Tillotson
Position within organisation	Ch/Supt Tactical Operations Command Kent Police
Signature	
Date of sign off	Reviewed 13/06/26

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?

Kent Police use drones in pursuit of meeting our Policing Purposes, which are 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

Drones are used for both planned tasks (e.g. operational planning) and in response to spontaneous incidents (e.g. searching for offenders or vulnerable missing persons, providing situational awareness to commanders during critical incidents), often in line with JESIP Principles with our emergency services partners.

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

Crime and Disorder Act 1998 - Implementing strategies to assist in 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 6 (Right to a fair trial), Article 8 (Right to Private Life), Article 10/11 (Freedom of Expression and Assembly).

Data Protection Act 2018 & GDPR - Kent Police handles data in compliance with these Acts to ensure the lawful and fair use of personal data.

MoPI Codes of Practice 2005.

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

Drones are a vital tool used in pursuit of the legitimate and lawful aim to fulfil our Policing Purposes as described above, and our Policing Duties: To detect, deter and disrupt criminality and increase public safety.

Drones are a proportionate and cost effective option for the provision of air support to policing operations, along with the National Police Air Service (NPAS). Drones are a good tactical option to meeting our duties in a measured, less disruptive and intrusive manner than alternative options.

-
4. Is the system being used for any other purpose other than those specified? If so please explain.

☐

Yes

☒

No

N/A

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

Action Plan

N/A

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?

A PIA was completed prior to May 2018, which was assessed and certified by the SCC. Since then, a separate data protection impact assessment (DPIA) has been completed in 2023 and reviewed and amended as required each year since then.

6. Have you identified any areas where action is required to conform more fully with the requirements of Principle 2? ☐ Yes ☒ No

Action Plan

Q2 - Drones are not used by Kent Police for facial recognition software or any other biometric recognition systems.

Q3 - A drone specific DPIA is in place, but will also sit under the overarching Kent Police DPIA.

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?

Any complaints regarding Kent Police's use of drones would be handled in the same manner, policies and processes as any other complaint. An initial complaint can be made in several ways, including direct, police station front counters, by phone, online, email etc. Advice on how to make a complaint can be found on the Kent Police website.

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

Action Plan

Q8/9 - This information is available on the Kent Police website, due to drones not being in a fixed location like a traditional CCTV camera.
Q10 - N/A to this specific form

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 use of drones at Kent Police falls under the governance of Tactical Operations Directorate who oversee the use of NPAS and drones within the Force. Drones also fall under the governance of the Tactical Operations SPR Board (Strategic Policing Requirement) which sits bi-annually. Kent Police also sits within both a regional Drones Working Group with the other South East Police Forces, and the NPCC APP Working Group, where best practice is established.

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>

A chain of command within Kent Police Tactical Operations is clearly defined, with the Strategic Lead Accountable Manager being the Tactical Operations Commander, and the Tactical Lead being a Tactical Operations Chief Inspector.

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?

All drone operators at Kent Police complete initial training before they are authorised to deploy a drone for Kent Police. This training includes their roles and responsibilities in terms of compliance with the legislative duties and purposes as described in the earlier Principles, and the definitions of overt and covert use of cameras to ensure they do not misuse drone technology. This knowledge and understanding is reinforced and tested during regular refresher training dates for all drone operators.

The operational use of drones is overseen under the governance of the Tactical Operations Directorate to ensure that policies and procedures are being maintained.

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

Q18 - N/A

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 Continual Professional Development (CPD) exercises and inputs take place, and Biannual Refresher Training and Assessment dates are in place, which all drone operators must attend and pass, for them to continue in this role. This training and assessment includes inputs and testing knowledge regarding policies and procedures for the correct handling of data obtained by drone.

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 drone operators must complete a CAA approved course from an authorised Nationally Qualified Entity listed by the CAA. This ensures that they have the required skills and knowledge to operate the system correctly.
All drone operators must maintain operational currency, of at least two hours deployment within a rolling three month period.
All drone operators must attend and pass annual refresher and assessment dates which provide inputs into policies & procedures, legislation and best practice, whilst also assessing this knowledge and practical demonstration of the required skill levels.

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

Operator ID: GBR-OP-8WTVGCGW4PXR

CAA Operational Authorisation: PDRA01-23887

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

☐

Yes

☒

No

Action Plan

N/A

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?

All evidential data is retained as required by MoPI Codes of Practice 2005, and in compliance with Policies and Procedures.
Any non-evidential data that does not meet a policing purpose is deleted after 31 days in compliance with MoPI Codes of Practice.

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

We have a Digital Assets Management System (DAMS) where this is done automatically against the classification of the data that is uploaded. This is using the same system that has been previously used by Kent Police for Body Worn Video, and therefore is a proven system.

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

N/A

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?

Access to data can be shared or limited as required using the DAMS system.

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 sharing of data is done via the secure DAMS system, which is designed and tested to be secure against security risks.

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

Any SARs in relation to drone data will be managed under current policies and procedures, such as Body Worn Video (BWV) procedures.

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 Kent Police website provides the public with information on the retention of data, access rights and procedures and information regarding FOI requests.

Data that is shared with 3rd party partner agencies is done in compliance with existing policies and procedures that would be the same as BWV.

42. Have you identified any areas where action is required to conform more fully with the requirements of Principle 7?

☐

Yes

☒

No

Action Plan

N/A

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 is ongoing work being completed by the NPCC to compile a National Catalogue of suitable drone equipment recommended for policing use.
The systems being used by Kent Police comply with this catalogue and have been selected to meet our operational and technical needs, whilst fitting within financial parameters with the view of drones providing cost reduction opportunities for the organisation.
The DAMS system used to manage data obtained by Kent Police drones has been selected as a result of several years worth of consultation and testing by other departments at Kent Police, including Procurement.

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

Standards are identified through continual horizon scanning and market research being compared against our operational needs and capabilities.

Procurement procedures are followed in the appropriate selection of drone equipment, and purchases are done so with competency and performance guarantees & warranties, and servicing agreements in place with the supplier.

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

N/A

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?

The systems used by Kent Police for the handling of data are encrypted between devices, and always in possession of an officer or kept secure if not in their possession. Once data is uploaded on to previously described DAMS, it is within secure police networks which are protected by extensive securities levels and firewalls. SD cards are reformatted to ensure that recorded data is not held outside of these secure systems once uploaded.

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?

Extensive security measures are in place, but will not be shared on this document.

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

CAA approved Operations Manual
SCC approved Policy and SOPs
SCC approved Data Privacy Impact Assessment
MoPI Codes of Practice 2005

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 systems used by Kent Police allow remote reformatting of memory storage.

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

N/A

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 use of drones is overseen by the Tactical Operations Directorate, and the Tactical Aviation Board which would include governance over the all systems meeting their purposes. As new best practice is identified, or improved technical systems available that offer improvements, these will be assessed and adopted/acquired where possible. We also sit within a Regional and National Boards where best practice is identified and shared.

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

N/A

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

Our drones are inspected before each use, and have a regular deeper inspection conducted to ensure the systems are maintained. In addition to this, they are serviced by a licenced third party, or sent away for repairs when a fault is identified to ensure the system remains safe and effective when used.

When not in use, drone equipment is stored in a secure room within a secure police building, which is temperature controlled to ensure they remain in good working order.

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?

The drone equipment used by Kent Police provide data that is in a format that fits within our (and partner) network and systems, and provides a high quality footage 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

N/A

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?

MoPI Codes of Practice 2005

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