

# 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](mailto: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 | Overt Public Order Evidence Cameras             |
| Senior Responsible Officer          | Ch/Supt Amanda Tillotson                        |
| Position within organisation        | Ch/Supt Tactical Operations Command Kent Police |
| Signature                           |                                                 |
| Date of sign off                    | 21/07/26                                        |

**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?

Public Order Evidence Gathering Officers deploy during public order operations in order to use overt video recording to reduce the risk of disorder and/or to aid identification of those responsible for criminal acts.

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

To overtly gather evidence of offences committed during public order operations. This is not designed as a Surveillance tool. The processing will be under the Law Enforcement Directive within Part 3 of the DPA 2018 in order to further the statutory obligations placed on Kent Police to prevent and detect crime

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

The deployment of officers operating overtly with video cameras is necessary and proportionate, as it is an essential tool used by police to support the legitimate aim of maintaining law and order during Public Order events and to support the prosecution of persons who commit criminal offences. Often such events attract hundreds if not thousands of participants and thus video recording is often the only viable way of gaining relevant evidence. The authorising officer will consider each application and the potential evidence that will be obtained by the use of such equipment. Authorisation for use should be considered as compelling, i.e. it is either the only or the most suitable tactic to be employed and must be proportional to the circumstances surrounding the use of video camera equipment. The Authorising Officer must ensure that the use of such equipment will not involve any unwarranted intrusion of privacy, and will be fully justifiable, proportionate and necessary in the circumstances of the incident or police operation.

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

☒

Yes

☐

No

Recordings taken for the purposes of briefings, contingency plans or training. Recordings of crime scenes, or other incidents, at the direction of a Scenes of Crime Officer, Senior Investigation Officer, Serious Collision Investigator or Crash Investigator.

- 
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?

No automatic facial or biometric recognition software used. The EGT capability is widely used across UK policing and has been in place for a number of years. It has the potential to gather the images of a large number of people, whilst also tracking an individual's behaviour and thus is a potential interference with qualified rights (eg, Article 8 ECHR – right to respect for private and family life). Overt filming raises significant human rights issues, notably the question of whether police action is compatible with the right to private life protected by ECHR Article 8. The Court of Appeal considered these issues in *Wood v Commissioner of Police of the Metropolis* [2009] EWCA Civ 414. Therefore, a DPIA is required under Data Protection Act 2018 - reviewed 2024.

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

☐

Yes

☒

No

**Action Plan**

N/A

### 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 concerns or complaints about the Overt use of video cameras, will be directed to the Professional Standards Department. When a complaint is known or anticipated then any footage will be retained.

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

#### Action Plan

N/A

## 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 Overt Use of Video Cameras is overseen by the Public Order Unit at Tactical Operations Command, and used in accordance with Kent Police force policy O26a, which details the overt use of video cameras by Police personnel. It is also supported by force policy W1000 and associated policies that provides guidance on information management, which underpins Kent Police legal, and national guidance and standards relating to information management. Policy S3000 applies to the management of Digital Evidence Seizure and Analysis.

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>

Publicised on Kent Police website.

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?

Public Order Evidence Gathering Officers complete refresher training each year and work alongside other trained officers where their roles and responsibilities are highlighted. Sussex Police hold the College Of Police (COP) Tactical Licence to deliver EGT training for the South East Region and conform to the National Police Public Order Public Safety Training Curriculum - Specialist Role Module F4. Moderation visits are conducted by the COP.

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**

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?

Public Order Evidence Gathering Officers complete refresher training each year and work alongside other trained officers where their roles and responsibilities are highlighted. Sussex Police hold the College Of Police (COP) Tactical Licence to deliver EGT training for the South East Region and conform to the National Police Public Order Public Safety Curriculum - Specialist Role Module F4. Moderisation visits are conducted by the COP. Relating policies are reviewed every two years.

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?

All operators have to undertake a Nationally Accredited training course.

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 operators have to undertake a Nationally accredited training course, licenced by the College of Policing. Moderation visits are completed by the Colleg of Policing to ensure compliance.

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?

BWV is governed by Policy 047 and the operational use of under SOP 047c.

---

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

☐

Yes

☒

No

N/A

---

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

☐

Yes

☒

No

**Action Plan**

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?

Recordings will be regularly reviewed in order to ensure that they remain necessary for a policing purpose and are adequate and up to date.  
Where the data provides evidence of an offence it will be retained in accordance with the Management of Police Information guidance which sets timescales dependent upon the nature of the offence.  
If it is reasonably anticipated that a complaint will be made but no offence is being investigated then the recordings will be retained for 18 months. If it is confirmed that no complaint will be made prior to the passing of 18 months, then the footage will be disposed of at that time. Non evidential & no reasonably anticipated complaint will result in the data being destroyed as soon as possible and in any case automatically within 18 months.

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

The footage uploaded to DAMS is stored within a retention category of 'Retain Complaint Likely' and has automatic deletion after 18 months.

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?

In accordance with SOP 026a the 'Disclosure Officer' or 'Investigation Officer' holds this responsibility who will review requests made to ensure access is for a legitimate and legal purpose.

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?

As per Kent Police Cyber security procedure as the retention of any images is on a Kent Police Encrypted Computer.

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

Application will be considered by the Public Disclosure Team and if appropriate a copy of relevant footage will be provided, appropriately redacted.

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?

Material will be shared with the the CPS for prosecution purposes or with another law enforcement agency to prevent and detect crime. All other disclosures are routed through the public disclosure team for appropriate assessment in line with the responsibilities under the DPA and the HRA.

---

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?

The standard video cameras used have been assessed as the required standard by Defence Science Technology Laboratories (DSTL)

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

The only video camera equipment to be used by Public Order Evidence Gathering Teams is from the Cannon XA camera series. Each out of the three divisions maintain two full live PO EGT kits for use only by nationally accredited Public Order Evidence Gathering trained officers. Details of this equipment are available from the Public Order Unit. Procurement of this equipment should be through the Public Order Unit (Tactical Operations Command) in consultation with business managers.

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?

Each camera uses a formatted SD card for initial recordings. Footage is then uploaded to DAMS. SD card is then formatted once upload completed. If DAMS not available then the footage is transferred from SD card to disc and sealed to protect evidential integrity and continuity of movement of this disc is recorded via Online Property Retrieval And Handling (OPRAH) system.

48. If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist?

☐

Yes

☒

No

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

N/A

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

Kent Force Policy O26a relates to this, as do the data protection policies under the overarching policy W1000.

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

N/A

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

N/A

---

53. In reviewing your responses to Principle 9, have you identified any areas where action is required to conform more fully with the requirements? If so, please list them below.

☐

Yes

☒

No

**Action Plan**

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?

Audited reviews of relevant policies and standard operating procedures.

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?

N/A

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?
- N/A
- 
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?

Force policy S3000, Digital Evidence Seizure and Analysis, applies to any video recording media that contains or may contain evidence. This policy contains advice and guidance on the viewing, handling, retention and disposal of all evidential video recording media.

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