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
Scope of surveillance camera system	Body Worn Video
Senior Responsible Officer	Supt S Inglis
Position within organisation	Force Intelligence
Signature	
Date of sign off	10th Dec 2019

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?

Allow the actions of police officers to be accountable and transparent. To increase the quality of evidence obtained by police officers through overt recording. To act as a visible deterrent in order to prevent crime and anti-social behaviour.
A revised force policy covering the use of Body Worn Video was signed off by the Force Executive Team on 21 October 2019. This policy gives guidance to officers and staff in relation to the use of devices and the system; and circumstances in which the use of Body Worn Video is appropriate.

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

Cameras are used in an overt capacity to enable police officers to record incidents, hence the provisions and restrictions of RIPA do not apply. To record interactions with members of the public, to obtain evidence that would otherwise be lost and therefore allow suspects of a crime a fair trial (Article 6 ECHR) and to reduce the time they are kept in custody unnecessarily (Article 5 ECHR). Common Law permits actions in the absence of any regulation prohibiting them.

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

Recordings are made when an officer believes that it is necessary and proportionate to gather evidence. This is largely for the officer to decide. The policy to allow officers to decide is in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. There are some circumstances where the use of BWV is mandatory - for example when carrying out stop and search or using force - and this is to protect the interests of both officers and members of the public who are subject to police actions. There is a formal policy in existence that covers the use of BWV within West Midlands Police.

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

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

Action Plan

No Action required.

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

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

☐ Yes ☒ No

Action Plan

No action required.

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?

Concerns and complaints are dealt with by the Force professional Standards Department, the Information Management Department or Legal Services Department, dependent upon the nature of the issues. The force website gives direction to members of the public who may be unhappy on how to complain, including how to complain online.

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

Action Plan

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?

There are force and regional governance meetings that is held quarterly in relation to all aspects of overt surveillance, including BWV. In addition there is a governance process of quarterly meetings in relation solely to the use of BWV and attended by all relevant departments.

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 details of the SRO (SPOC) are included on the OPCC's external website along with this SAT.

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?

The Body Worn Video policy details roles and responsibilities and these are reinforced in training that is delivered to officers and staff. The system, devices and processes are subject to ongoing audit and compliance checking, both centrally and by line managers.

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

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?

We have SPOCs and cascade trainers across the force who are there to ensure that the camera system is used correctly and to provide refresher training wherever it is needed.

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?

N/A - Our users are police officers who are trained in the use of cameras.

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?

There are mandatory circumsatnces in which a camera MUST be used - as detailed in policy. Otherwise it is at the officers discretion, however it must be for a defined policing purpose.

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

This will be covered in the WMP Drones self-assessment.

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

☐ Yes ☒ No

Action Plan

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?

Footage is stored by our cameras on a digital system - Evidence.com, supplied by Axon (the system supplier). All evidence is stored by default for 31 days before automatic deletion, unless marked for a longer period of retention by an investigating officer. This is enough time to ensure that if it is required for an investigation it is saved. All footage that is saved for longer than 31 days is saved in line with the principles of the Management of Police Information (MoPI) to be available for disclosure purposes.

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

The software that stores the images/videos will automatically delete the footage after the relevant retention period has expired.

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

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?

General access to the system is limited to police officers and staff. Within this, there are 3 levels of access.
Users who may see their own footage only (restricted to camera users)
Users who may see all unrestricted footage (supervisors, administrators and investigators)
Users who may see all footage. or all footage within a given category (professional standards investigators, firearms authorisers, homicide and child abuse).
Third party access to footage is allowed through subject access requests, only for footage showing that individual and only after it has been redacted to remove all other persons' identifiable details.

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?

Cameras are encrypted with 256 AES levels of encryption, data stored in the cloud is encrypted to the same level.

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

A member of the public can make a Subject Access Request online, via the force website.The request is processed by a dedicated team who will identify the relevant videos and redact identifiable features of anyone who is not the requesting person. This includes both images and sound.

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?

There is an agreed protocol with the Crown Prosecution Service, who are the partner agency that footage is shared with as part of the criminal justice process.

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

Action Plan

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?

College of Policing Approved Professional Practice.

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

Force Policy, and monitored by the establisged governanace process. Ongoing support and maintainance are provided by the Force IT & Digital support department.

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

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?

Access to the system requires a usename and password. Access to the system is IP address restricted to ensure that data can not be accessed from outside the West Midlands Police infrastructure. The cameras themselves are encrypted to prevent access to the footage if a physical device is obtained by an unauthorised person.

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?

Passwords and usernames as well as an IP whitelisting system

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

Through Evidence.com - access is restricted as detailed above, and instructions given during initial training and awareness sessions. Guidance is also available on the Force intranet.

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?

The cameras are encrypted.

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

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?

Governance meetings and ongoing BAU monitoring. Surveillance Monitoring meetings also consider the use of the system and help to shape force policy, which remains subject to periodic review. Use of BWV is also integral to regular force scrutiny meetings looking at stop & search and use od force and is considered during those meetings, both locally and through the auspices of the Office of the Police & Crime Commissioner.

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

Use of BWV is subject to ongoing review in relation to the benefits gained from the use of the system - in terms of financial savings and gains for the force in terms of securing best evidence for use in criminal proceedings, increased legitimacy and enhanced accountability. Currently there are no other viable options to achieve the same aims.

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

Support contract in place with Axon and ongoing action by Force IT & Digital Department.

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

Action Plan

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?

Liaison with CPS.

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?

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