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 speed enforcement cameras. Average, Variable and Mobile
Senior Responsible Officer	Simon Inglis
Position within organisation	Superintendent - Force Intelligence
Signature	
Date of sign off	01/12/22

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 speed enforcement cameras to reduce excess speed and casualties on our roads

Cameras are deployed on roads with issues of excess speed or casualties that have data to back up that requirement.

West Midlands Police work closely with partner agencies and deploy accordingly, using DFT Guidelines, NPCC Guidelines and manufacturers guidelines and operating procedures.

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

Local Orders, Section 84 and 89 (1) of the Road Traffic Regulation Act 1984 & Schedule 2 to the Road Traffic Offenders Act 1988 amended by the Road Traffic Act 1991.

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?

West Midlands Police deploy speed enforcement cameras to reduce excess speed and casualties on our roads

Cameras are deployed on roads with issues of excess speed or casualties that have data to back up that requirement.
This method of enforcement is the least intrusive way of achieving our objective.

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

We do assist with providing intelligence for murder enquiries and serious crime for WMP from any of our camera resources

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 do not use automatic facial recognition software or biometric characteristic recognition systems

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 implented and then refered to the Department of Professional Standards if required to do so and investigated in line with Force Policy.

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

Action Plan

A seperare 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

Claire Waring is the Single Point of Contact. We have our own internet page which is called wmsafetycameras.co.uk which gives out information about our work and data around our enforcement locations.

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 camera operator receives specific training in relation to the use of the camera and its technology. This specific training is delivered either by an external company or now can be delivered by another member of staff who has received a trainer trainers course and is able to deliver the same level of training. Specific training is also provided for the software that is used to enforce the cameras.

The team work well together and there are guides on where the locations are and parking positions etc. Any issues are also highlighted to supervision and management.

Regular updates are also provided to the team should any changes to legislation become known and also if there are any changes to processes.

Letters from the public asking for images or questioning their offence can sometime highlight issues but in general issues are highlighted and rectified by regular dip samples undertaken by supervision and management

NCALT packages for WMP training is also completed by all staff.

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?

WMP conversations are a time where an understanding of the role is questioned and any issues highlighted and updated.
We also complete a DIP sample process of the work conducted to ensure that the cameras are being used in the correct manner.

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 camera operators are trained by the camera manufacturer and certificated as necessary once competent. There is also a member of the team who has been trained as a trainer to ensure that competency levels are managed and can offer advice as necessary. The rules and guidance about the standards of camera operation
All back office equipment receives thorough training from the camera manufacturers and then cascade training is also provided.

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

Not applicable

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?

Images are on our software system for approx 2years but we do keep copies of all enforcement discs for 6 (plus the current) years. This is because members of the public can appeal sentences at court and also advice was sought from forensic services on how long we shoud retain images and they advised 6 years (plus the current) under the rules of MOPI

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

After each deployment the camera operator erases their flash cards for use again. They do however retain all their work on the copy disc (as above). The images that are captured and saved on our back office software and erased by IT after 2years

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?

Camera operators and camera enforcement staff have automatic access to images as part of their roles. We have officers and PSIs who utilise those images for any enquiries that may take place such as pervert the course of justice cases.
Our central ticket office also has limited access to the back office software package with the images available. The software package is password controlled.
Members of the public who have a ticket are entitled under the rules of disclosure to see their offence image. This is sent out to them via the postal system. Not via email.

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?

Our images are kept on a secure network that IT have overall control of.

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

As described above, all members of the public are entitled to see their offence images. They would need to write in or call in with this request. They need to give the reference number of the offence, and their full name and address details for us to cross reference the details. Family members are not entitled to call on behalf of someone else. The named person on the NIP must be the person who requests the images.
Internal intelligence requests are done by email so that an audit trail of requests can be kept

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.

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

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?

For our cameras there are manufacturers standards and guidelines. There are also the NPCC and DFT guidelines and each cameras has to be Home Office Type Approved before it can be used in any enforcement circumstances

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

Each operator has recognised training delivered by either the manufacturer or the in house trainer we have in the department. They are also provided a copy of all the guideance documents. Each camera is required to be calibrated every 12 months, failure to do so will make any enforcement illegal and no NIPs are allowed to be sent if the camera is out of calibration. The calibration can only be completed by the manufacturer.

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?

The software that is used within the department is password secured. This password is gained from the manager of the camera enforcement unit. The Central Ticket Office and some CMPG officers also have access but read only. Once offences are copied onto discs, they are then secured in envelopes with a security seal which us recorded on an audit sheet. They are filed in a cabinet in a locked room. That locked room is also in an office with a coded lock on the door

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?

WMP IT infrastructure 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?

Guidelines are in place from NPCC, DFT and Manufacturers as well as an induction paperwork for all new staff
Code of Practice on the Management of Police Information (MOPI)

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?

Not Applicable

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?

All locations are risk assessed for suitablity. This includes yearly speed surveys and yearly check on casualty stats. Based on these the stats, the sites are graded, Red Amber, Green and White. Once a site becomes White it is no longer a priority. It will still be seen by the team but on a reduced basis to ensure that the resource is being used for the correct circumstances.

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

Local Authorities may see that the location needs engineering work rather than enforcement. This is a joint collaboration based on stats shared.

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

Each camera can only obtain Home Office Type Approval if they are regularly maintained and calibrated by the manufacturer.

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?

Unsure on how to answer this one as this relates to home office type approved equipment and therefore we have no stakeholder arrangements for this.

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?

Not Applicable.

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

If someone has committed an offence of excess speed.

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.