

# 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.

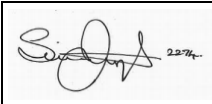
## What should I do next?

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](mailto: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	Automatic Number Plate Recognition (ANPR) - Vehicle Mounted
Senior Responsible Officer	Simon Inglis
Position within organisation	Superintendent
Signature	
Date of sign off	26/03/26

**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?

The National Police Chiefs Council ANPR strategy and the West Midlands Police ANPR strategy clearly identifies why we use ANPR technology;

- Increase public confidence and reassurance;
- Reduce crime and terrorism;
- Increase the number of offences detected;
- Reduce road traffic casualties;
- Increase efficiency of police resources.

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

The management and use of ANPR must be in accordance with the provisions of National ANPR Standards for Policing and Law Enforcement (NASPLE) that provide detailed safeguards to ensure that the use is lawful and consistent with the requirements of legislation.

The legal basis for ANPR is established by reference to the Data Protection Act 2018, Common Law and is implicit from the Protection of Freedoms Act 2012 that includes requirements for law enforcement use of ANPR to comply with the Surveillance Camera Code of Practice.

ANPR technology is in daily use by law enforcement and other agencies in the United Kingdom. Its use falls within three primary categories: to identify vehicles of interest and operationally respond; gather intelligence and further police capability to investigate crime.

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

The policing purposes outlined for each individual camera deployment demonstrate a lawful basis for the processing of ANPR data at Common Law, in that the use of the data is both pressing and proportionate in the circumstances. ANPR technology is in daily use by law enforcement and other agencies in the United Kingdom. Its use falls within three primary categories: to identify vehicles of interest and operationally respond; gather intelligence and further police capability to investigate crime and it is in this context that this deployment is considered. This is the least intrusive way of meeting the objective.

---

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**

None

## 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

In relation to question 2, we do not use facial recognition or biometric character recognition.

### 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?

The West Midlands Police website, including within the ANPR section provides details and allows members of the public to make a complaint online. This will then be processed by West Midlands Police including involving both the ANPR Manager and ANPR senior officer lead.

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

#### Action Plan

The West Midlands Police website contains all of the information required to comply with principal 3 of the code.

## 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 West Midlands Police ANPR Policy clearly outlines the governance structure for ANPR. In addition, West Midlands Police fully engage and participates with the national and regional governance of ANPR use by police with representatives at both regional and national level.

West Midlands Police also hold a bi-monthly overt surveillance board chaired by an SRO. West Midlands Police also actively participate in both regional and national overt surveillance groups.

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 single point of contact is the ANPR Manager who will liaise as necessary with the strategic and senior officer leads for both ANPR and the senior responsible officer for overt surveillance.

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 West Midlands Police ANPR policy is available to all staff on the intranet. All users of ANPR systems have to undertake computer based training, including that on NASPLE (National ANPR Standards for Policing and Law Enforcement), policy and procedure including passing a test on these standards. Additional face to face training is provided for force owned ANPR systems.

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**

None

## 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?

The NASPLE (National ANPR Standards for Policing and Law Enforcement) and West Midlands Police ANPR policy and strategy are made available to all users of the ANPR system. Use of the ANPR system is also subject of audit.

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 users must complete College of Policing approved computer based training and pass a test on their competence and understanding prior to being allowed access to the NAS system. All staff also have to meet NASPLE vetting requirements prior to been granted access and have vetting reviewed to maintain access.

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

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?

ANPR data is retained within the NAS (National ANPR Service) in line with current requirements of the NASPLE (National ANPR Standards for Policing and Law Enforcement). This is currently 12 months. In addition, ANPR data is also held within the West Midlands Police ANPR Management server for 7 days as required under NASPLE.

ANPR data is also retained for 12 months in the West Midlands Police BOF (Back Office Facility).

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

Both the NAS and BOF routinely delete images and data each day that becomes 12 months old.

The Management Server likewise, daily deletes all images that reach 7 days old.

This is a fully automated process.

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**

None

## 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 ANPR data is in line with NASPLE. This is also reflected within the West Midlands Police ANPR policy.

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 ANPR system is contained within the West Midlands Police IT network along with other policing systems. Information security is under constant monitoring and review and is subject to PEN test and internal and external scrutiny.

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

All subject access requests will be processed by the Freedom of Information team within West Midlands Police Information Management department. The team will engage with the ANPR Manager to obtain information and ensure that all legal obligations and timelines are complied with.

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?

Disclosure of ANPR data is processed in line with NASPLE (National ANPR Standards for Policing and Law Enforcement). To ensure the strict policy is followed, only a small number of appropriately trained staff are authorised to produce ANPR material for disclosure. All disputes over disclosure are reviewed by the ANPR Manager who will engage senior officer leads if and as required. All staff who complete the computer based training are informed of this as part of the training and have to accept a written statement confirming they will not disclose ANPR data prior to being granted access.

---

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

Yes

No

**Action Plan**

None

## 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?

West Midlands Police is striving to ensure that all ANPR cameras deployed comply with the standards set down within the NASPLE (National ANPR Standards for Policing and Law Enforcement).

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

All vehicle mounted ANPR cameras are covered by a support and maintenance contract to ensure they are maintained appropriately. This support includes specialist engineers attending site at least once per week to conduct both reactive and pre-emptive maintenance to ensure continued operation.

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

None

## 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?

National ANPR Standards for Policing and Law Enforcement outlines the access to ANPR data, and these are strictly adhered to. ANPR Data is treated as restricted data and stored in accordance with national guidelines. Access to the data is restricted to staff who require it and then is subject of individual login with relevant permissions assigned to their job role. Access is removed from a staff member who no longer requires access due to role change. There is a full audit capability for all use.

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?

The ANPR systems is contained within the West Midlands Police IT network along with other policing systems. Information security is under constant monitoring and review and is subject to PEN test and internal and external scrutiny as part of the police network certification.

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

National ANPR Standards for Policing and Law Enforcement outline all procedures and guidelines regarding the storage, use and access to ANPR data. The NASPLE is re-enforced by the West Midlands Police ANPR Policy.

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**

None

## 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?

Police vehicle mounted ANPR cameras are subject of data protection impact assessments. These are annually reviewed to ensure their use remains necessary and proportionate.

Vehicle mounted ANPR is fitted to some police vehicles, all of which are subject to bespoke daily tasking into high threat, risk and harm areas. This tasking is under constant review which ensure that vehicle mounted ANPR is deployed appropriately.

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

No

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

All components of the system are subject of maintenance, either externally via a specialist ANPR supplier or internally through West Midlands Police IT & Digital department. Critical system components are subject of 24/7 maintenance.

All cameras are operated in line with the National ANPR Standards for Policing and Law Enforcement requirements.

58. Have you identified any areas where action is required to conform more fully with the requirements of Principle 10?

Yes

No

### Action Plan

None

## 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 National ANPR Standards for Policing and Law Enforcement provide the guidance which is followed by West Midlands Police. Key stakeholders internally are IT & Digital and Information Management. Both departments are represented at the ANPR project boards.

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

None

## 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?

Automatic Number Plate Recognition technology is used to help detect, deter and disrupt crime at a local, force, regional and national level. It allows the police to tackle travelling criminals, organised crime groups and terrorists.

ANPR provides lines of enquiry and evidence for crime investigations and is used by forces throughout England, Wales, Scotland and Northern Ireland, including West Midlands Police.

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

The main reference database for ANPR is PNC, the Police National Computer. The national PNC policy outlines when police interest markers should be added to vehicles and what type of markers should be added dependent on the severity and type of reason for the police interest.

West Midlands Police holds additional reference databases on its ANPR system, all of which are operated in line with the National ANPR Standards for Policing and Law Enforcement.

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?

National ANPR Standards for Policing and Law Enforcement and West Midlands Police ANPR Policy.

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**

None