

Self Assessment Tool

How well does your organisation comply with the 12 guiding principles of the Surveillance Camera Code of Practice? Complete this easy to use self assessment tool to find out if you do.

Using this tool

This self assessment tool has been prepared by the Surveillance Camera Commissioner (SCC) to help you and your organisation identify if you're complying with the [Surveillance Camera Code of Practice](#) (the Code). It should be completed in conjunction with the Code, and can help to show you how well you comply with each of its 12 guiding principles.

It is possible to be largely compliant with some principles and to fall short against others. As a result you will note that at the end of the questions against each principle there is a space to include an action plan. This is so you can put actions in place over the next year to improve your compliance to that principle. These boxes can also be used to make a note of what evidence you could produce if required to show your compliance to that principle.

The template contains a combination of open and closed questions. For the open questions, there is a limit on how much you can write within the template, so please feel free to include any additional notes as an annex to the document – there are additional blank pages at the end of the tool to help you to do so.

Remember that your organisation may operate more than one surveillance camera system, with a scope that extends across several purposes and many geographical locations. So, before you start clarify the scope of the system(s) you propose to self assess for compliance against the Code.

Is this tool for me?

The self assessment tool is aimed primarily at relevant authorities under [Section 33 of the Protection of Freedoms Act 2012](#) who have a statutory duty to have regard to the guidance in the Code. In general terms, this means local authorities and the police in England and Wales.

If you work within any other organisation that operates surveillance camera systems you are free to adopt and follow the principles of the Code on a voluntary basis. If you decide to do so, then using this tool will be of benefit to you.

As a relevant authority under Section 33, if you are considering the deployment of a new surveillance camera system, or considering extending the purposes for which you use an existing system, you may find the more [detailed three stage passport to compliance tool a valuable planning tool](#). It can guide you through the relevant principles within the Code and inform you of the necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the Code.

If you are from any other organisation operating a surveillance camera system you may find this template useful in reviewing your use of surveillance, or may want to use other SCC online tools such as the [Data Protection Impact Assessment](#) guidance or the [Buyers Toolkit](#) to help decide whether your surveillance is necessary, lawful and effective.

What should I do next?

The self assessment is for you to satisfy yourself and the subjects of your surveillance that you meet the 12 principles and to identify any additional work necessary to show compliance. Think about realistic timescales for completion of your action plans, with a view to achieving full compliance with the Code before undertaking your next annual review.

The SCC does not want you to submit your completed self assessment response to him. However, in the interest of transparency he encourages you to publish the completed self assessment tool template on your website.

A completed self assessment is also a positive step towards [third party certification](#) against the Code.

Email the SCC at scc@sccommissioner.gov.uk to let us know when you have completed this template as this will enable us to understand the level of uptake. We would also appreciate your comments and feedback on the user experience with this template. Please let us know if you are interested in working towards third party certification against the Code in the near future, or would like to be added to our mailing list.

Name of organisation	Northants Police
Scope of surveillance camera system	280 static ANPR camera sites 35 ANPR equipped cars 10 Rapid deployment cameras Back office software and associated database
Senior Responsible Officer	D/Supt Lee McBride
Position within organisation	Superintendent Proactive Crime & Intelligence
Signature	
Date of sign off	

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 force regularly updates a Strategic Camera Assessment. It provides recommendations for the siting of ANPR cameras in Northamptonshire based on an analytical assessment in 4 areas; 1. National Security and Counter Terrorism, 2. Serious/organised/Major crime, 3. Local crime, 4. Community confidence and reassurance, crime prevention and reduction.

Camera locations are scored against the 38 recommendations in these areas to ensure that each has an identified objective towards the pressing need.

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

ANPR operates under a complex framework of legislation of general application, including the General Data Protection Regulations (GDPR), the DPA, the Surveillance Camera Code and Common Law. The National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Surveillance Camera Commissioner (SCC). ANPR data from police forces is police information within the meaning of The Code of Practice on the Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997. It is shared in accordance with the provisions of that Code. Access to and the retention and management of ANPR data obtained is compatible and consistent with their relevant legal obligations, which include:

- Data Protection Act 2018, Part 3, Chapter 1, Section 31 - 'The Law Enforcement Purposes'
- ICO Code of Practice for Surveillance Camera Systems (ICO Code of Practice for Surveillance Camera Systems (ICO Code));
- College of Policing Approved Professional Practice – Information Management. (MOPI);
- Part 2 of the Protection of Freedoms Act 2012 (PoFA);
- The Surveillance Camera Code issued under Part 2 of PoFA.
- Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA);

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

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.

The management and use of ANPR must be in accordance with the provisions of NASPLE that provide detailed safeguards to ensure that the use is lawful and consistent with the requirements of legislation. The management and use of ANPR cameras deployed as a result of this assessment will be in compliance with those requirements.

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

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?

n/a - the DPIA is necessary and has been completed.

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

Action Plan

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?

There is a complaint page on the force website at address <https://www.northants.police.uk/advice/advice-and-information/c/complaints/what-is-a-complaint/>
There is also a link to this page at www.northants.police.uk/ANPR

Complaints can be recorded over the phone, in writing, or online via the website. These are processed and dealt with by the Office for Police Fire & Crime Commissioner as detailed on the website

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

Action Plan

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?

Designated Strategic Lead at Superintendent level responsible for chairing a quarterly Strategic ANPR Group attended by internal stakeholders, which covers updates on ANPR related projects, compliance with national standards, updates on infrastructure, and budgets.

The ANPR Manager is the tactical lead the runs ANPR for the force on a day to day basis. The ANPR Manager chairs a bi-monthly tactical group attended by operational users from various departments. This covers the finer details such as VOI lists, use of car kits, performance capture.

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>

Supt Hillery is SPOC for overt surveillance. Details on ANPR page on force 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?

An ANPR Manager has been appointed to provide oversight of all ANPR processes and compliance with NASPLE and the Audit Standards. Authorised users of ANPR are only granted access to the data to the extent that is necessary for their role and are required to successfully complete training, dependant on their role and responsibilities. Their training record is reviewed prior to permissions being granted.

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?

On induction to the system, or upon increase in system permissions, the user is delivered a uniform training package. User accounts will be locked or removed from the system after a period of time and user will have to make contact with administrator in order to regain access. At this point any training needs are established. For Northgate BOF, accounts are deleted after a period of 6 months inactivity, for NAS accounts are auto-locked at 90 days of inactivity. BOF will be phased out over the next year, leaving NAS as the sole system.

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?

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?

As per above all users will undergo training on use of the ANPR system. This compliments all training the officer or staff member has already had such as law training, data protection, and MoPI for example. User transactions are auditted and any training needs will be identified through this process.

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

Principle 6

No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

30. How long is the period for which you routinely retain images and information, and please explain why this period is proportionate to the purpose for which they were captured?

All images and information are routinely retained for 12 months to support police investigations. This retention period is in place nationally as a result of a paper published by NPCC 18th October 2017 "Review of Automatic Number Plate Recognition (ANPR) Data Retention Period" Author CC Charlie Hall. This paper is evidence based and details the level of access to the data seen by UK police forces. The retention period was reduced in 2018 from 2 years to 1 year following the review to ensure the amount of data stored is proportionate to its processing activity. Data captured in Northamptonshire is available to support investigations in all UK police forces and approved LEAs.

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

Images and information are stored for the purpose of prevention & detection of crime, and the apprehension or prosecution of offenders, as per Data Protection Act 2018, Schedule 2, Part 1(2).

The retention period for ANPR data was reduced to 1 year on 1st April 2018 in accordance with national guidelines.

Unless preserved for an investigation, all data will be deleted after this time unless it is preserved in line with provisions of Criminal Procedure and Investigation Act (CPIA) 1996.

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

Regular review process needs implementing for data retained past 12 month weeding under CPIA rules.

The data and principles will be aligned to the Information Commissioners Office/Information Asset Ownership guidelines in particular around RRD assessment. Regular dip sampling is being implemented and a review will be completed in terms of progress at the quarterly strategic meetings

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?

Only trained staff (with at minimum RV vetting status) can access data stored within the system.

Only a limited number of users have access to search more than 90 days (from the date of search) of data, this is based on the role of the user. Users with over 90 day search access have been provided NASPLE guidelines that pertain to how serious an offence needs to be in order to search longer timeframes.

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?

All logins and login attempts are logged within the system, and NASPLE Audit 8.2.2 mandates repeated unsuccessful login attempts are investigated.
The ANPR system is within the secure police network.

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

We have an Information Unit that deals with all legal requests from members of the public such as subject access requests, and freedom of information requests. Details are on the Northants Police website.

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?

All data sharing from ANPR system is within confines of NASPLE, specifically Section 5.1, which defines the legal basis for the sharing of information.

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?

The National ANPR Standards for Police & Law enforcement (NASPLE).

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

When a new camera/system is installed it shall be tested in accordance with technical standards within NASPLE standards (Part 2). Tests and other technical requirements will be conducted by supplier on install, and will be conducted by force ANPR Field Engineer on ongoing basis.

All other aspects of ANPR in force are audited in accordance with NASPLE Audit & Compliance document. This is monitored by the national ANPR Auditor.

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?

All images are stored in a database on secure police network. Access to these images are only possible through front end BOF or NAS software

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 server that directly connects to cameras at the side of the road sits in a 'de-militarised zone' (DMZ) meaning it offers further security protection and does not leave the core police network vulnerable to external threat. All other ANPR systems sit within the secure police PSN network which is regularly reviewed and audited in accordance with NPIRMT requirements. the force holds current and valid GIRR 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?

The force is compliant with NASPLE Part 3: Data Access and Management Standards, and NPCC ANPR 'Use of data for evidential and intelligence purposes'. The force ANPR policy reflects both of the above documents, and informs users how national guidelines are complied with at a local level

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

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?

Yearly strategic assessments are completed, which the camera estate is scored against to ensure all cameras continue to be deployed for a stated policing purpose. Data Protection Impact Assessments are completed when there are any changes to the system, which is signed off by the designated Senior Information Risk Owner (SIRO)

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

Alternative tactical options are recorded in DPIA

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

Force employs an ANPR Field Engineer who maintains the cameras and ensures requirements in national standards are met

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?

Northgate was the first back office ANPR system ever used when ANPR was first used for law enforcement around 25 years ago. The format of exhibits produced from the system has been used for this period of time and is nationally recognised as admissible. NAS is a new national system; stakeholder engagement has been undertaken in the formation of the Evidence Working Group which comprises of subject matter experts from police forces and approved law enforcement agencies across the country with guidance and support from the Crown Prosecution Service. The main aim of the EWG is to ensure national consistency in relation to evidence produced from NAS. Part of this is that the documents exported from the system (specifically the format and content of the witness statements for England & Wales, and for Scotland) are compliant with Criminal Procedure Rules, r 27.2; Criminal Justice Act 1967, s.9; Magistrates' Courts Act 1980, s.5B and also the Government Security Classifications.

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

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?

ANPR technology within Northants is used to help detect, deter and disrupt criminality at all levels including tackling traveling criminals, Organised Crime Groups and terrorists.

Real time sightings are compared against VOI lists and if there is a match an alarm is sent to the 'Alarm Stack' which is monitored in the Control Room and by officers on patrol.

Data collected from the cameras is stored and can be accessed for up to a year to provide lines of enquiry for police investigations.

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

Vehicles linked to police intelligence, vehicles that have been involved in the commission of crime, or vehicles associated with a person with safeguarding concerns are included in ANPR hotlists. There is a human review process in between the intelligence being received and it being put on the ANPR system.

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?

All vehicles included in VOI lists will not stay on the system longer than 28 days without review in accordance with NASPLE 8.13.6.

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