SURVEILLANCE CAMERA COMMISSIONER

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	Leicestershire Police
Scope of surveillance camera system	ANPR Camera system
Senior Responsible Officer	Kerry Smith
Position within organisation	T/ACC and Force Senior Information Risk Owner
Signature	
Date of sign off	August 2022

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?

Leics Police ANPR cameras are deployed to address the issues of national security, serious, organised and major crime, local crime, for crime prevention, detection and reduction purposes and also to in crease community confidence and reassurance. These aims and objectives are written in a Force ANPR Strategic Assessment. This strategic Assessment is reviewed on a yearly basis.

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: Compliance with the Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA));. Processing will be conducted under part 3 of the DPA 2018, for law enforcement purposes so that Leicestershire Police can further its statutory obligations • 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?

Our ANPR cameras are justified under the Human Rights Act as necessary and proportionate and are deployed in the interests of national security, public safety, the prevention of crime and disorder and the protection of health. They are used to help detect, deter and disrupt criminality at a local, force, regional and national level.

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

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

P 2 Q2-Leics Police don't use automated facial recognition for ANPR.

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?

All police forces have a complaints procedure that is fully available on the force website. This is for all complants not just ANPR. The website provides details about what a complaint is, how a complaint can be made, how we investigate a complaint etc.

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

Action Plan

P3 Q8-signage not used as this could lead to criminals avoiding ANPR cameras. However there is an ANPR Fact Sheet attached to the force website that explains why ANPR is deployed.

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?

Extensive vetting and training is completed prior to being allowed access to the ANPR system. Access to the ANPR system is restricted and is based on need. The hotlist use, cameras and camera timings are checked by the ANPR manager on a regular basis .Additionaly, should an authorised person not use the system within a defined period then they will be informed that their access could be suspended if their need for the system has ceased. ANPR data is securely stored and retained in accordance with NASPLE guidelines. Leics Police has adopted the 12 month data retention policy afterwhich the system will auto delete the data.
To ensure that any access to, use of and / or removal of data from the ANPR system is necessary and proprtionate, the system is regularly monitored and audited in line with the National Standards for the compliance and audit of law enforcement ANPR.
The Force also has an ANPR Policy and Procedure in place that is available to all users.These documents are reviewed on a regular basis. If and when there are any updates or changes relating to ANPR, this is communicated Force wide via an article published on the Force's internal website so that all users are aware of any developments etc.
The Senior Responsible Officer for ANPR in Leics is the Assistant Chief Constable.

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 / senior responsible officer for surveillance camera governance arrangements is Leicester Polices Director of Intelligence currently Detective Superintendent James Avery. Leicester Polices 'How we use surveillance cameras' webpage has details on the deployment of surveillance cameras and contact details of the single point of contact / senior responsible officer

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 Force ANPR Procedure outlines how ANPR in Leics is used. All users of the system are required to complete and pass at least the Basic User NCALT training package before being allowed access to the ANPR system. In addition certain searches require a authorising officer. Monitoring,auditing and compliance checks of ANPR searches are completed by gatekeepers.

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

Auditing TVM is not currently undertaken due to no current provision in force. However, staff have just been recruited within Data Protection to start conducting audits. At this time discussions are taking place regarding what this will look like and will commence shortly after.

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 Force ANPR Procedure is regularly updated and a Latest News article is published to all staff stating it has been updated and requesting they read it. User auditing of searches also takes place to ensure their compliance.There are National Standards for compliance and audit of law enforcement ANPR, that also requires Leicestershire Police to produce periodic reports for the national auditor. The ability to produce certain documents such as Intelligence Reports and evidential statements is also restricted to only certain members of staff with certain depts.

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?

Basic Users are required to undertake NCALT (VLE) training prior to being allowed access to the system. In more specialists roles such as an Intelligence Analyst, advanced training is completed in a classroom environment.

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?

As per the National ANPR standards for Law Enforcement, the ANPR data retention period is one year. Records can be retained for longer if it is identified that there is a policing purpose to retain thos records for evidential purposes eg CPIA. If data is asked to be retained, a request can be made to the Intelligence Admin Team who retain the data and keep a record. After a set period of time the officer making the request will be contacted to establish if the data needs to be retained any longer.

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

The ANPR system is set to "auto delete" data after 12 months unless retained.

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?

In order to access the ANPR system, an officer will need to justify an operational need to search the database. NASPLE guidelines are followed in this respect. If a request to have access to the system is authorised, a mandatory training package is issued to the uset to complete. If a person without a user authority requires a small number of ANPR searches to be completed, an ANPR search request form with the relevant authority, is required to be completed.

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 Force has a comprehensive firewall in place to prevent cyber attacks to its systems. Any ANPR Data that is disclosed is done so under NASPLE and CPIA disclosure rules and only when it is required evidentially or part of an intelligence product. Evidential packages are sanitised to only include the vehicle/s in question, approximately where the vehicle has been recorded and the time and date that vehicle has been recorded. Any intelligence products disclosed are classified as Restricted.

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

SARs are processed through the Forces Information Management Dept.Any requests for information from ANPR systems will be directed to them in the first instance.

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 Force has a variety of Information Sharing Agreements with other competant agencies/authorities such as Trading Standards. In such circumstances and where ANPR is concerned, an agency can make a request for intelligence held in relation to a specific vehicle. If the request is justified, legal and necessary a search of ANPR will be carried out over a specified time frame. Any results obtained will be released back to the requesting

agency via an Intelligence Report. If that agency then requests an evidential statement, one will be provided.

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

Action Plan

There are currently no restrictions on BOF2 access.

Ensure that Force Privacy Notice (FPN) includes ANPR as a data Source as together with other National Websites for ANPR, this publicises to Data Subjects that their data may be captured by this method The FPN will also inform Data Subjects of their access rights.

Add to the Procedure documents for ANPR that any Subject Access request for ANPR is forwarded to the Information Management Depratment for processing / response

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 System (NAS) introduced a series of standards with regards how ANPR is used/managed. This is called NASPLE. Once achieved forces will be accredited. These standards take into account the ICO Codes of Practice, the Surveillance Camera Code, CPIA Code of Practce and the Code of practice for the Management of Police Information. We are continually working to ensure compliance with those standards.

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

A reviewed and updated Force ANPR Procedure documenting newly added requirements/standards, renewed training procedure has been rolled out for the NAS and a new ANPR Delivery Plan has been created for a number of key areas of business within ANPR. Increased auditing and monitoring will be conducted in line with national requirements.

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

Auditing TVM is not currently undertaken due to no current provision in force. However, saff have ust been recruited within Data Protection to start conducting audits. At this time discussions are taking place regarding what this will look like and will commence shortly after.

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?

Extensive firewalls exist to safeguard the system and data held. Users of the ANPR systems are required to complete training packages before gaining access. Training also covers the obligations under Data Protection and associated legislation. In addition, only specially trained staff are authorised to create evidential packages. To ensure the intergrity of the read data and images obtained by ANPR, all camera reads are frequently audited / checked and calibrated as per NASPLE. Detailed maintenance logs of the ANPR cameras are also kept as required under the National Standards for compliance and audit of law enforcement ANPR

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?

Police Digital Service, to assure this, with this process supplemented by an annual penetration test of our environment, alongside internal processes such as the use of vulnerability management software to routinely scan our environment and remediate any vulnerabilities identified. The Force also benefits from the protections afforded by Office 365 utilising a number of these tools to safeguard our environment, with safeguards in place to safeguard our on-premise environment such as perimeter safeguards, encryption, anti-virus/anti-malware tools etc. The Force have a close working relation with the National Management Centre, who provide a number of services to Forces – protective monitoring, cyber threat intelligence and remediation advice etc.

Robust security incident management processes are in place within the Force and documented within bespoke procedures (both Cyber and traditional security incidents). An escalation process is in place to ensure that notification occurs to the relevant stakeholders within a timely manner, and within the legislated timeframe.

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

MOPI (management of Police Information) Force ANPR Procedure and NASPLE documentation

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

Nil

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?

The Force ANPR Procedure documents such things. This document will be reviewed annually to ensure it still complies with NASPLE and auditing requirements. Under the forces Overt Surveliance Board the mechanisms of ANPR are reviewed regularly. The DPIA is also reviewed on a regular basis.

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

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

A small number of staff oversee the management of the ANPR system. Any faults are quickly reported and if it cannot be rectified, a service engineer will be requested.Maintenance agreements are in place with a 48 hour response time.

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

Action Plan

At this time auditing TVM is not currently undertaken due to no current provision in force. However, staff have been recruited within Data Protection to start conducting audits. At this time discussions are taking place regarding what this will look like and will commence shortly after.

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?

There has been community consultation on ANPR, most recently in 2021 via social media. On that occasion over 5000 responded and the majority were in favour of ANPR deployment for the reasons outlined.

Consultation also took place with key departments who will need an evidential product from ANPR. Consultation also took place with the CPS around the presentation of evidence, disclosure of evidence and CPIA.

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?

Full use of ANPR.

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

Vehicles of interest that are suspected to be connected to issues of national security, serious, organised and major crime, local crime, for crime prevention and reduction purposes can be added to a hot list.

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?

Leics Police adhere to national guidance and retain data for 12 months unless retained for a specific reasons eg evidence and CPIA

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