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	CCTV FHQ (including Dogs). L Turnidge CCTV Tigers Road (Covert Site). L Turnidge SARC Juniper Lodge - M Gant - Seperate DPIA The Lighthouse - DCI Fletcher - Separate DPIA Custody Suite CCTV. Separate DPIA EPAC CCTV. Separate DPIA EMSOU - TBC
Senior Responsible Officer	Robert Nixon
Position within organisation	Temporary Chief Constable
Signature	
Date of sign off	22 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?

CCTV systems protecting force personnel and premises require a DPIA. This self assessment should help identify risks to be mitigated against.

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

The lawful basis is detection and prevention of crime and Leicestershire Police comply with all relevent legislation including data protection legislation, Human Rights Act, Equalities Act and Surveillance Commissioners Code of Practice

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

Police personnel both staff and officers are a potential target from disgruntled members of the public, criminals and terrorists. The use of CCTV on Force owned sites provides an additional layer to the protective security measured employed.

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

Access control to restricted areas which includes evidential property and controlled substances.

The CCTV that covers the Police Dogs compound is also used to assist with monitoring animal welfare and security.

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

Action Plan

On completion of the CCTV DPIA, separate annexes should cover any additional sites that the Police have responsibility over the data. The Police have a number of CCTV systems with Partner Agencies, these must not be overlooked and are listed on page 2 of this SAT

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?

We have not. DPIA is being 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

Updated signage around the Force estate will commence 8 August onwards.
Complete DPIA for CCTV on site, comment in DPIA should include that our systems do not use facial recognition technology. DPIA to be a live document and reviewed regularly and when fundamental changes are made to the system.

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?

Any concerns or complaints firstly go to the Security Manager who escalates to the Information Manager as necessary. Escalate to PSD if required.

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

Action Plan

Check that privacy notice signage includes the purpose for which CCTV is in use. Also who operates the system, POC for further information. New signage now produced and a works schedule to replace signage starts 8 August 22.

A check of our Privacy Statements needs to be done to ensure CCTV, purpose etc is included. Privacy Notice being updated 26 July 22.

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?

CCTV is strictly controlled by the Security Team. Any requests for access need to be directed to them. Their line management has changed to the Information Manager who can respond to any Data Protection issues. He reports directly to the SIRO.

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

This is included in our privacy statements. With both a Data Protection Officer - Steven Morris and a Senior Information Risk Owner (SIRO) DCC.

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 Security Manager has daily oversight of the security team and has regular contact with his line manager. Both the Information Manager and Deputy Information Manager spend time with the security team to review practices and procedures.

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

Update policy and procedure documents once DPIA is completed. Current P&P with security team as part of their contract. CCTV is over written every 30 days. Access requests only come from PSD with an e-mail first as an auditable trail. Access requests monitored by Security Manager. SPOC for CCTV will be Aiddy Simpson - Security Manager. Produce a procedure document that covers capture, access, deletion, roles and reposibilities. This already exists and is with Security in their instructions. However this is scheduled for review 29 July 22.

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 security team receive security training. The security teams line management goes to the Data Protection Officer who is able to provide bespoke training on Privacy issues. They do not need a CCTV licence as working on a private site (not open to the public). Contractors and visitors do attend site so additional signage will be adopted at entrances.

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?

Two members of the security team.

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?

Trained by Security Manager and/or Deputy Security Manager.

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?

BWV is not used by the security team.

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

Drones are not used by the security team.

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

☐ Yes ☐ No

Action Plan

Update P&P once DPIA is completed.

Ensure that any policies and procedures are covered in any induction process for anyone joining the security team.

No monitoring of public spaces is conducted, only on premises surveillance is carried out by those with the appropriate SIA licenses.

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?

30 days. The system overwrites itself and it is determined that a crime would have been reported within this time frame.

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

Set up by our IT department.

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

N/a

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?

Our Professional Standards Department confirm who has access. Any retained images are requested by PSD, isolated by the Security Manager, retained until a nominated person collects. Images are deleted once PSD confirms that the original is no longer required for their investigations.

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?

Information is retained internally only

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

SARs come to the Information Management Dept. If a request is made suitably trained staff deal with the request and liaise with PSD and security as required.

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?

We do not disclose to a third party. If it was evidential for a criminal investigation the data would still be retained internally until the casefile is submitted to the courts. Other control procedures are then followed to safeguard the data.

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

Action Plan

N/a

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?

System conforms to ISO 27001. All Force projects need to be approved by the Force Information Security team. All new members of staff will have a Workplace Induction Programme (WIP) that will cover CCTV use.

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

The CCTV contract ensures that appropriate techical updates are completed.

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

Review policy and procedure documents and amend any areas that are not clear. Make sure viewing public spaces and appropriate use are included. Scheduled for review 29 July 22.

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?

Isolated system behind our Firewall. Only accessible by security team. Requests for info go through an approved request procedure that starts with an e-mail from PSD, which gives an auditable trail.

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?

IT Cyber Security provide the latest patching and penetration testing. The wider network has to be secure for annual accreditation and health checks are conducted annually. The data in the CCTV system is isolated behind that protection.

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

Procedural documentation covers all processing and access permissions. This is referred to as the assignment instruction.

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

Policy and procedure paperwork must cover who can access data and have an auditable trail for requests.

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?

Necessary - Unfortunately the threat against staff is unlikely to reduce, so the system is likely to be required for the foreseeable future.
Proportionate - Once a DPIA is completed the proportionality will be reviewed annually.

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

Cameras are an integral part of a layered protective security system. It complements foot patrols and increases the ability to monitor the site.

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

The system has regular maintenance from the provider Reflex. All issues are reported immediately and issues are reported to Information Management and IT. On going issues move to a risk register within the SSD for tracking and completion.

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

Action Plan

DPIA required and an annual review to ensure the proportionality aspect is considered.

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?

Data is not exported. In terms of evidential standards the security team liaise with PSD which ensures the standard is to the correct level. If at any point the standard changes then Information Management will be required to produce a business case to upgrade the system.

61. Do you have safeguards in place to ensure the forensic integrity of the images and information, including a complete audit trail? ☒ Yes ☐ No

62. Is the information in a format that is easily exportable? ☒ Yes ☐ No

63. Does the storage ensure the integrity and quality of the original recording and of the meta-data? ☒ Yes ☐ No

64. Have you identified any areas where action is required to conform more fully with the requirements of Principle 11? ☒ Yes ☐ No

Action Plan

N/a

Principle 12

Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

65. What use do you make of integrated surveillance technology such as automatic number plate recognition or automatic facial recognition software?

ANPR is not linked to the CCTV - Though this is under review
No automatic facial recognition software is used.

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

Vehicles require a pass to be on site. Linking number plates to owners will assist with knowing who is on site and when. Particularly important at periods of minimum manning such as evenings and weekends.

67. Do you have a policy in place to ensure that the information contained on your database is accurate and up to date? ☐ Yes ☐ No

68. What policies are in place to determine how long information remains in the reference database?

N/a as the database linked to ANPR does not exist yet.

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

However if ANPR gets linked to the CCTV system then a review of the DPIA will be required. This may mean updating privacy statements, signage and additional control measures over the maintenance.