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	Norfolk Constabulary
Scope of surveillance camera system	CCTV cameras attached to mobile vehicles with linked Live Facial Recognition software (NEC Neoface) attached, which will capture images of all persons who walk within designated zones and cross refer to a pre-populated watch list of specific identified persons of interest.
Senior Responsible Officer	ACC Julie Dean
Position within organisation	Assistant Chief Constable
Signature	
Date of sign off	18/03/26

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?

Live Facial Recognition (LFR) is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces against a predetermined watchlist and generates an alert when a possible match is found.

LFR can be a valuable policing tool that helps forces keep the public safe and to meet their common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

The following are illustrative examples where LFR may assist Forces achieve their policing purposes:

• supporting the location and arrest of people wanted for criminal offences.

• supporting the location and arrest of people outstanding for warrants.

• preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders)

• supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc)

• supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

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

Data Protection Act 2018, Pt 3, Ch 1, s.31: Law Enforcement Processing. UK-GDPR, Art 9(2)(g) Public Task and Data Protection Act 2018, Schedule 1, s18

Suffolk and Norfolk's Constabularies Legal Mandate sets out all of the statutory legislation and common law judgments being relied upon in the use of Live Facial Recognition.

Key common law powers the Constabularies may rely on when utilising LFR technology include the policing common law powers to act to:

(a) protect life and property;

(b) preserve order and prevent threats to public security;

(c) prevent and detect crime;

(d) bring offenders to justice; and

(e) uphold national security.

The above information is held within our LFR Legal mandate.

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

Any deployment is fully inline with the College of Police Authorised Professional Practice on Live Facial Recognition. The deployment will be targeted, intelligence led and both time and geographically limited. All relevant persons added to the watchlist fit the criteria set out within the Force Policy including those wanted by the courts; and/or suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or missing persons deemed increased risk; and/or presenting a risk of harm to themselves or others.
To ensure proportionality against the rights and freedoms of members of the public not part of the watchlist, the deployments will be advertised in advance of the dates of deployment. There will be information and signage in the area to explain to members of the public that LFR is being used. The intrusion may be perceived as being high, but the information / images captured will be automatically checked against a pre-prepared watch list. If there is a match, officers will look to interact the person identified. If there is no match, the image and data will be destroyed immediately in less than a second and not stored.

The above information is covered in further detail within our LFR Policy document and DPIA.

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

No other areas for action have been identified.

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 - DPIA 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

No other areas for action have been identified.

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?

Engagement officers will be able to engage with the public during deployments to allay any concerns.

Suffolk and Norfolk Constabularies also ensure that members of the public can make complaints on the phone, in person in their local station, by post or online as per the public complaints process. A dedicated LFR email inbox has been set up for general enquiries.

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

Action Plan

No other areas for action have been identified.

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 use of LFR by Suffolk and Norfolk Constabulary is set out in the LFR Policy, LFR Procedure, the DPIA and Legal Manadate.
Any deployment of LFR will be in line with the governance processes set out within the procedure documentation.

Post Pilot any ongoing use of LFR is governed through a board process led by the Senior Responsible Officer (SRO)

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 will be the Authorising Officer having considered their role and the command structure for the deployments.

Contact will be via the compliance email address and this is published on the privacy notice and LFR page. Multiple signs with links/QR codes will be at the deployment so contact details will be easily available. Officers will be briefed to advise this if asked.

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?

No deployment of LFR can happen without authorisation from the Authorising Officer who will ensure compliance with all policy and procedure. All relevant staff are made aware of the roles and responsibilities relating to the LFR system. Training is delivered to all officers who are to partake in LFR deployments.

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

No other areas for action have been identified.

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 LFR system will only be operated by trained staff in designated roles. Training and ongoing support is obtained via the supplier. The ongoing use and operation of LFR is governed through a board process which will ensure that all operational, technical, privacy considerations, policies and procedures are up to date and fit for purpose.

For the purpose of this pilot we are utilising trained staff in designated roles in BEDS Police through Mutual Aid.

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?

Operators are all warranted police officers with relevent training and experience in using the system.

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 cameras will be utilised in line with current force Policy which covers when to activate BWV recording which includes the 30 second pre recording function.

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

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

☐ Yes ☒ No

Action Plan

No other areas for action have been identified.

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?

The CCTV feed will be stored for a maximum of 31 days unless further retention is justified in line with current retention schedules. Biometric templates of those that generate an alert from the watch list will be deleted within 24 hours. Biometric templates of those who do not generate alert on the watchlist will be deleted immediately.

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

The application/software will automatically delete biometric templates of those who do not generate an alert. Those who generate an alert will be deleted after 24 hours. The CCTV will automatically be deleted after 31 days.

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

No other areas for action have been identified.

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 those with approved access and trained to use the LFR CCTV system will have access to the retained CCTV. This is governed by our IT access approval processes.

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 entire system has been subject to the relevant ISO and IT security measures and assurance. The data processed in any deployment is used by Suffolk and Norfolk Constabulary only.The LFR system is air-gapped from any external systems.

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

Subjects can make a Subject Access Request for a copy of their personal data held by Suffolk and Norfolk Constabulary. The biometric template is not an image, and will be deleted within 24 hours. The custody image used for addition to the watchlist will be retained in line with MoPI guidance and therefore can be requested through the SAR process here - Ask for information about yourself | Norfolk Constabulary

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?

No information from the LFR system will be shared with a third party. If for any reason there is a need to share the CCTV imagery with a third party this will be in line with force policy, CPIA or any other statutory legislation requiring the disclosure of the images

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

☐ Yes ☒ No

Action Plan

No other areas for action have been identified

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 deployment and use of the CCTV and LFR technology has undertaken rigourous testing independently by the supplier, Beds Police. There are applicable ISO standards. In particular we conform to: ISO / IEC 30137-1:2024.

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

The system is owned by Beds Police after being provided by the Home Office under a National LFR roll out programme. The entire system is fully assessed by Beds Police IT, Information Security and Data Protection professionals. These standards are continously monitored and reviewed. We ensure that the accuracy of the Live Facial Recognition is fit for purpose through testing against the ISO standard (see above link) and optimising system configuration parameters in line with this standard and NPL guidance.

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

No other areas for action have been identified

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?

Only approved authorised users will have access to the images. The CCTV system and LFR software is fully auditable on user actions and access. The CCTV recording is maintained for 31 days and then deleted. Any LFR watchlists are deleted from the system at the end of the deployment. Any LFR match images to the watch list are deleted at the end of deployment or within 24 hours, any biometric image of a data subject captured that doesn't feature on a watchlist will be deleted immediately.
The LFR systems are stand-alone. Data is encrypted prior to upload.

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 system is owned by Beds Police. The entire system has been fully reviewed and assured by Beds Police and Home Office IT and Information Security to the required standards. This is held within the high level design of the system and the Information Security Baseline Security Assessment. The LFR systems are stand-alone. Data is encrypted prior to upload.

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

This is all documented within the Force Policy, Procedure, Legal Mandate and DPIA.

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?

Existing procedures in place will be followed in relation to BWV cameras being lost or stolen which replicates if this should happen in day to day regular duties.

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

No other areas for action have been identified

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?

Any use of LFR technology will be managed and reviewed through a FR Technology board and working group process with key stakeholders ensuring all current and future requirements are met along with regular review periods of Policy.

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

The inclusion on a watch list requires the Authorising Officer to consider if less intrusive methods have been considered.

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

The system in owned by Beds Police. They monitor this through ongoing reviews and maintenance process by operational teams, IT and the supplier NEC.

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

Action Plan

There are no areas of further action required.

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 imaging from the LFR system is not evidential. The notification of a suggested match must still be reviewed by an officer and any decisions thereafter on engagement is that of the officer dealing.

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

There are no areas of further action required.

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?

There is no integrated ANPR cameras included in this deployment. This deployment is solely use of live facial recognition software and no other.

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

The reference database or 'watchlist' has been devised ensuring that it is both proptionate and relevant to the deployment. The inclusion of an image of a watchlist is as per the criteria set out in Principle 1 section 3 and LFR Policy document.

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?

The Force policy, procedure and Authorising Officer Policy Decision cover the managing of the deployment, data and retention.

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

There are no areas of further action required.