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	Sussex Police and Surrey Police

Scope of surveillance camera system	Sussex Police and Surrey Police (hereafter referred to as Sx/Sy Police) will be deploying standard CCTV cameras attached to mobile vehicles with linked Live Facial Recognition (LFR) software attached. The LFR vans will capture images of all persons who walk within designated zones and extract a biometric template of the facial features which is then compared against a pre-populated watchlist of images of specific identified persons of interest (being individuals wanted on warrant, recalled to prison, on suspicion of the commission of serious or priority crime or high-risk missing persons). If further use cases are considered in the future, this assessment will be refreshed. Any image scanned which does not flag a potential match is automatically and almost instantaneously deleted. The originating CCTV images are not retained by police. Forces have released extensive websites to ensure lawful and transparent processing, these are available: www.sussex.police.uk/police-forces/sussex-police/areas/au/about-us/governance-and-processes/live-facial-recognition/ www.surrey.police.uk/police-forces/surrey-police/areas/au/about-us/live-facial-recognition/
Senior Responsible Officer	
Position within organisation	Assistant Chief Constable
Signature	
Date of sign off	08/10/2025

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?

At any time, Sussex Police and Surrey Police (hereafter referred to as 'Sx / Sy police') are pursuing enquiries to locate and arrest large numbers of suspects including for priority offences, such as domestic abuse. Sx/Sy police also manage significant numbers of missing persons and are required to monitor and enforce criminal justice and civil prohibition orders. It is necessary to make these enquiries as prompt and efficient as possible to maximise public safety and effective resource management. The use of Live Facial Recognition (LFR) will contribute to this objective by supporting real time investigations to locate and engage with persons of interest.

The Forces will deploy LFR for the purposes outlined below:

- 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

- high risk missing persons (subject to specific parameters) who present a serious risk of harm to themselves or others.

- police and court-imposed orders - such as football banning orders, stalking prevention orders, etc.

Full details regarding the overarching justification for the deployments can be found on the public facing Force websites. These ensure transparancy with the public and detail Forces intentions to utilise LFR as well as disclosing the LFR Policy, Standard Operating Procedure (SOP) and LFR Application and Authorisation process for deployments.

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

Processing of personal data for law enforcement purposes is conducted in accordance with Part 3 of the Data Protection Act 2018, in particular section 35(2)(b) Data Protection Act 2018 where the processing is necessary for a task carried out for a law enforcement purpose by a competent authority for the purposes of the Act. The definition of a function for 'law enforcement purposes' covers activities that are for the 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public

security.

Sensitive processing for law enforcement purposes is carried out in accordance with section 35(5) Data Protection Act 2018 and only where one or more of the following conditions apply for processing that is necessary:

- for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest [Schedule 8 paragraph 1];

- to protect the vital interests of the data subject or of another individual [Schedule 8 paragraph 3];

- for the safeguarding of children or individuals at risk [Schedule 8 paragraph 4];

Where processing takes place pursuant to the UK General Data Protection Regulation (UK GDPR), such as for the puporse of locating high risk missing persons, processing will meet one or more of the following conditions where processing is necessary:

- to protect the vital interests of the data subject or another natural person [Article 6(1)(d) UK GDPR];

- for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6(1)(e) UK GDPR].

Where processing special category data, it will meet one of the following conditions where processing is necessary:

- to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Article 9(2)(c) UK GDPR];

- for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject [Article 9(2)(g) UK GDPR]

Processing will also and meets one or more of the following conditions of Part 2 Schedule 1 Data Protection Act 2018 and an appropriate policy document is in place (this will be published on the Force internet pages to ensure transparency:

- the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 6] in the case of high risk missing persons, this will relate to the Force's duty under Article 2 ECHR to preserve life;

- and/or processing is necessary for the purposes of safeguarding children and individuals at risk [Part 2 Schedule 1 paragraph 18].

Deployments are also subject of an Equality Impact Assessment and Human Rights Impact Assessment to confirm their compliance with the Equality Act 2010, the Public Sector Equality Duty (PSED) and the Human Rights Act 1998.

To esnure compliance with transparency, signs publicising the use of LFR will be prominently placed in advance (both outside and within) the zone of recognition to alert members of the public to the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the zone. The public will also be notified (where possible) in advance of the Deployment and details will uploaded to public facing websites and other appropriate communication channels (potentially including social media).

Members of the public who are subject to an engagement following an LFR alert will also be offered information about the technology and how to make further enquries.

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

In connection with individuals wanted for Law Enforcement purposes, there continues to be high levels of individuals who have not been located through traditional policing methods. It is therefore necessary, both in the sense of responding to the pressing social need to tackle serious, violent and other priority crimes and in the sense that less intrusive alternatives have been tried but have failed/not been sufficiently successful.

In relation to high risk missing persons, being individuals who pose a risk to themselves or others, it is in their interests as well as those of society that they are located and safeguarded as soon as practically possible.

A range of measures have been implemented to not only ensure but to demonstrate that the deployments will be proportionate, including: specifying and targeting the categories of individual who may be included on the Watchlist; conducting deployments overtly, advertising them in advance and providing information to the public to ensure that deployments are transparent; specifying and targeting the locations at which LFR may be deployed.

Measures are in place to ensure that the data being processed is minimised and its retention is limited to the shortest reasonable period; a retention period has been implemented in connection with the CCTV images collected; and, the efficacy of the LFR system as well as the potential for bias and discrimination have been subject to scientific testing and the Sx/Sy Police LFR Software DPIA specifies the minimum configuration thresholds for the deployment which ensure equitability.

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 further 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?

No

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?

Sx/Sy Police already has in place and publishes information regarding where to direct general police complaints as well as data protection specific complaints through publication of relevant team contacts and the Data Protection Officer (DPO).

In connection with the LFR Deployments, Sx/Sy Police has implemented a route of recourse and individuals will be able to direct complaints (or any other feedback) regarding the deployment of LFR to an email account. This is publicised online and is also proactively provided to individuals who are subject to an engagement.

The email account will be triaged by the Force Leads who will send any requests or complaints to the appropriate handling departments, including data subjects exercising their Rights.

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?

There is a Senior Responsible Officer (SRO) board that has operational oversight of all aspects of the use of facial recognition in Sx / Sy Police. This is chaired by ACC rank and ensures governance is addressed at all stages of the LFR usage. The proposed use of LFR has also been presented and discussed at senior management boards within both Forces.

The data protection documentation has been reviewed and approved by Data Protection Officers (DPO) and Strategic Information Risk Officer (SIRO) to ensure compliance with governance requirements. LFR documentation has also been reviewed by Sx / Sy police legal representation to ensure it is compliant with legal requirements before obtaining SRO approval.

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 Points of Contact (SP0C) and Subject Matter Expert (SME) for each Force are detailed in the internal policy documents. Each force has an email address which is publicised on posters (lfr@surrey.police.uk and lfr@sussex.police.uk).

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?

All individuals involved in LFR will be briefed on their role and the importance of exercising independent judgement before each deployment. This includes staff involved with the watch list generation, the software operator in the van and officers engaging with the public (whether for a hit or general challenges to LFR). All requirements are fully detailed in the SOP and staff are expected to read this prior to deployment to ensure their understanding remains current and relevant. There is also a Superintendant or above authority required for each deployment.

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?

All individuals involved in an LFR depoyment will receive training in advance as well as a briefing on the day of the deployment. Training includes requiring them to understand the nature, limitations and sensitivies of the use of LFR, as well as the Sx/Sy Police LFR documentation in so far as is appropriate to their role.

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?

All staff accessing the LFR software have undergone training.

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?

LFR Operators have received specialist training and have appropriate operational experience.

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?

This is fully detailed in the SOP. Although officers will receive specific training for LFR engagement, they are also required to adhere to current processes for activation of BWV devices under Force policy. Any engagement where the Officer approaches a member of the public following a LFR hit / review will be recorded on Body Worn Video for evidential purposes.

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

Not relevant as no drones.

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 further areas of concern are 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 not be stored, this will be real time processing only. Any biometric templates that do not generate a hit on the LFR system will not be stored. Any hits that generate a LFR potential match will be retained for a period of 24 hours only and manually deleted by the operator.
Any engagment with the data subject will be recorded on Body Worn Video for evidential purposes, there is no necessity to retain the match data as it has been verified by the operator.
Watchlist images uploaded to the system and transferred to the system via encrypted USB memory stick are deleted from the LFR system and USB stick within 24 hours of the deployment.

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

The LFR system will automatically delete biometric templates of those who do not generate an alert. Any hits that generate a LFR potential match wil be retained for a period of 24 hours only and manually deleted by the operator.

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. Retention periods have been implemented to ensure there is no extended processing of personal data through the use of LFR and therefore the data is not re-purposed for any other law enforcment purpose.

Principle 7

Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

36. How do you decide who has access to the images and information retained by your surveillance camera system?

Access to biometric data and CCTV images are privileged. The generation of the watchlist is restricted to specific staff who, on clear instruction from the approved governance processes, will run the specified algorithm to extract targeted biometric templates. These will be stored on an encrypted USB stick that will be accessed by the LFR operator only.

The watchlist data will be extract the watchlist directly into the LFR software in the van, at which point the watchlist will be deleted from the USB stick. The watchlist data is only retained for a short period of time, this being the active deployment as it is not anticipated that further use would be feasible.

Once imported, the watchlist and associated biometric templates will only be accessible to the LFR operator, therefore ensuring necessity of access to a restricted number of users.

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?

As stated in Q36, there will be no additional processing of the watchlist data other than for that specific live deployment. All police systems holding images are subject to regular Information Security assessment to ensure protection of the data held within, this includes compliance with mandated IT Healthchecks for all software systems.

Specifically, the LFR NeoFace software is a siloed non-networked system which is subject to security measures, this includes restricted access and is only accessible to trained staff to upload and view the watchlist data. The LFR software has full audit functionality to ensure compliance in accordance with section 62 Data Protection Act 2018.

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

Sx/Sy Police has established policies and procedures on handling data subject access requests, Freedom of Information Act requests and Rights to Be Forgotten / Rectification. These are serviced via email requests and via forms on the Force internet sites. Any relevant information held at the date of the request relating to the individual will be considered for disclosure.

The below pages have been published to ensure transparency with data subjects. The pages will be updated with deployment and decision updates for the use of LFR. These sites will also serve as a pro active Freedom of Information (FoI) dislcosures.

• Live Facial Recognition | Sussex Police (www.sussex.police.uk/police-forces/sussex-police/areas/au/about-us/governance-and-processes/live-facial-recognition) • Live Facial Recognition | Surrey Police (www.surrey.police.uk/police-forces/surrey-police/areas/au/about-us/live-facial-recognition)

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?

It is not anicipated that Sx / Sy will share any LFR information with third parties.

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 LFR software is NEC NeoFace, this has been purchased and implemented on the LFR vans nationally which means all Police deployments of LFR utilise this software. The systems have been tested by the manufacturers to ensure there is no demographic and gender bias. The current LFR software has undergone commissioned evaluation by the National Physical Laboratory.

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

Hardware and software have been Nationally commissioned following a thorough procurement process. This also ensured all software was thoroughly tested for bias and all Forces had detailed compliant governance in place surrounding deployments and transparency.

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

There are no additional actions required.

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?

Watch list data is transferred from Sx/Sy Police systems to the standalone LFR system via an encrypted USB memory stick. The stick is required to be securely wiped within 24 hours of the deployment.

The LFR system itself is a siloed non-networked system, which is subject to security measures. Logging data is retained of user activity in accordance with section 62 Data Protection Act 2018 which enables auditing to be conducted.

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?

See question 47 response.

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

See response to Q36. A SOP has been created that addresses all stages of the LFR process, from authorisation to deployment. This also addresses the current restrictions on the creation, extraction, processing and deletion of the data in the watchlist to ensure it is only retained for the necessary period. An operational decision was made not to retain the CCTV footage from the deployments, this ensures no further processing of the data for compatible law enforcement purposes. Therefore the only access is limited to the specific deployment. All decisions and processes are recorded as part of the project review and within the SOP.

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?

Not applicable.

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?

There are existing Force protocols to manage this and ensure the security of the device and the footage held within. These are well established processes and external to the LFR deployment. There is also a Force Data Breach policy that includes loss of media and

hardware devices.

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?

Sx/Sy police are currently trialling the use of LFR to evaluate the efficiency and results of using this method of policing. As such, the deployment of LFR by Sx / Sy Police will remain under regular internal and external review throughout the period of proposed deployments.

If the LFR demonstrates a justifiable benefit for law enforcment, it will be subject to periodic review including staff guidance, watchlist thresholds, external publications, post deployment evaluations and public perception.

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 Sx/Sy Police LFR Policy and SOP, as well as the DPIA and other LFR documentation detail the alternative, less-intrusive measures that have been tried and failed prior to the consideration of the deployment of LFR.

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

National procurement of hardware and software has ensured sufficient maintenance and review of all software and hardware for LFR deployments.

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

Action Plan

No other areas for action have been identified.

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?

Stakeholder engagement with Sx/Sy Police technical teams during the design of a script to extract images for the Watch List from Niche. There are specific criteria for all Watch Lists that will be agreed prior to any deployment and will have Asset Owner approval.

The effectiveness of scripts will be tested for extraction accuracy.

LFR is being deployed as an intelligence tool to locate persons on the watchlist. In the unlikely event that the presence of an individual in a recognition zone becomes materially relevant in an investigation, the Authorising Officer will consider whether any relevant LFR data should be used as evidence and a decsion made jointly between Sx/Sy Police and the Crown Prosecution Service.

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

No other areas for action have been identified.

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?

As detailed above, the LFR system involves the extraction of a biometric template from a Watch list image and compares that to templates extracted from CCTV images of individuals passing through the LFR zone of recognition.

As set out in the Sx/Sy Police LFR Policy, SOP and other LFR Documentation, the importance of the quality of source images is recognised and subject to specific guidelines.

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

There are specified categories of individual who may be included on a Watch list. These ensure that only relevant and necessary persons of interest are inlcuded specific to that deployment area. Watchlists are confirmed no earlier than 24 hours prior to a deployment to ensure their currency.

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?

Information held on police systems is subject to the College of Policing Authorised Professional Practice on Information Management and other court decisions. Mechanisms are in place in accordance with the Sx/Sy Police Policy and SOP to ensure that only lawfully held images are considered for inclusion in an LFR Watchlist. No other areas for action have been identified.

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

No other areas for action have been identified.