# 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 | Hampshire & Isle of Wight Constabulary |
| Scope of surveillance camera system | Standard CCTV cameras attached to mobile vehicles with linked Live Facial Recognition software attached, which 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, outstanding suspects for a range of criminal offences, including high risk crimes and those relating to local district priorities which justifies the inclusion, or missing persons considered at increased risk of harm assessed as high or medium risk) from which a biometric template has already been extracted. Any image scanned which does not flag a potential match is automaticlaly and almost instantaneously deleted. The originating CCTV images are retained by policing for at least 31 days and a longer period if required, for example: if required as evidence in an investigation / prosecution or is needed to investigate a received complaint about officer conduct. |

| | |
|---|---|
| Senior Responsible Officer | ACC Paul Bartolomeo |
| Position within organisation | Assistant Chief Constable - Crime and Criminal Justice |
| Signature | Paul Bartolomeo |
| Date of sign off | 09/12/25 |

## 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?

HIOWC has identified several hotspots for high risk and priority crime and has taken efforts to tackle these including conducting the Home Office funded Operation Sentinel. While this saw a reduction in criminality, this has not resulted in significant reductions in criminality including violence. A separate operation, Operation Relentless, focused on outstanding warrants has some limited success but has not resulted in any long term impact on the number of warrants that remain outstanding across the county. Furthermore, in circumstances where individuals go missing and pose a risk of harm to themselves or others it is imperative that those individuals are identified and safeguarded at the earliest opportunity.

HIOWC has therefore identified several areas where it proposes to deploy Live Facial Recognition (LFR) technology in an effort to tackle these types of crime in locations and on days and times at which intelligence suggests incidents have occurred previously.

The purpose of the deployments is to locate persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison, to locate individuals who are designated as a current high risk and medium risk missing person, to locate suspects wanted for a range of criminal offences, including high risk crimes and those relating to local district priorities which justifies inclusion on a watchlist; with a view to apprehending and prosecuting offenders, preventing and detecting crime and supporting the administration of justice. In relation to high-risk and medium-risk missing persons, they are sought to be identified for safeguarding purposes.

Further detail regarding the overarching justification for the deployments can be found in the HIOWC LFR Policy and Standard Operating Procedure (SOP) and for specific deployments in the relevant HIOWC LFR Application and Authorisation.

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

Details of the lawful basis for the use of surveillance are set out in the HIOWC Legal Mandate but, in summary, the use of LFR by the police for law enforcement purposes has been confirmed to fall within police powers at common law by the Court of Appeal in R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058.

Processing of personal data for non-high risk missing persons is conducted in accordance with Part 3 Data Protection Act 2018, in particular section 35(2)(b) Data Protection Act 2018, i.e. the processing is necessary for a task carried out for the law enforcement purposes by HIOWC, which is a competent authority for the purposes of the Act. Sensitive processing is carried out in accordance with section 35(5) Data Protection Act 2018 and

one or more of the following conditions will apply: 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 [Schedule 8 paragraph 1]; processing is necessary for the administration of justice [Schedule 8 paragraph 2]; processing is necessary to protect the vital interests of the data subject or of another individual [Schedule 8 paragraph 3]; processing is necessary for the safeguarding of children or individuals at risk [Schedule 8 paragraph 4]; processing relates to personal data manifestly made public by the data subject [Schedule 8 paragraph 5]; and/or processing is necessary for the purposes of or in connection with legal proceedings [Schedule 8 paragraph 6(a)].

Where processing takes place pursuant to the UK GDPR, processing will meet one or more of the following conditions: processing is necessary for compliance with a legal obligation to which the controller is subject [Article 6(1)(c) UK GDPR]; processing is necessary to protect the vital interests of the data subject or another natural person [Article 6(1)(d) UK GDPR]; and/or processing is necessary 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 concerns special category personal data, processing will meet one of the following conditions: 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]; processing relates to personal data which are manifestly made public by the data subject [Article 9(2)(e) UK GDPR]; and/or processing is necessary 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] 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: 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]; the processing is necessary for the administration of justice [Part 2 Schedule 1 paragraph 7]; processing relates to a specified category of personal data and is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained [Part 2 Schedule 1 paragraph 8]; processing is necessary for the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as to not prejudice those purposes and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 10]; processing is necessary for the purpose of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act [Part 2 Schedule 1 paragraph 12]; and/or processing is necessary for the purposes of safeguarding children and individuals at risk [Part 2 Schedule 1 paragraph 18].

The deployments have also been the subject of an Equality Impact Assessment and Human Rights Impact Assessment to confirm their compliance with the Equality Act 2010 and HIOWC's compliance with the Public Sector Equality Duty (PSED), and the Human Rights Act 1998.

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

As set out above, and in more detail in the HIOWC LFR Policy, SOP, Application and Authorisation which should be read in conjunction with this Assessment, HIOWC has duties to prevent and detect crime but, notwithstanding the demonstrable efforts such as Operation SENTINEL there remain stubborn locations at which serious and priority crime continues and which have not been significantly reduced by traditional means. In connection with individuals wanted on warrant, there continues to be high levels of individuals wanted on outstanding warrants and 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 and medium 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 adavance 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 most sensitive 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 HIOWC LFR Policy and SOP specify the minimum configuration thresholds for the deployment which are at levels at which equitability is secured.

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**

Having regard to the HIOWC LFR Documentation, and in particular the HIOWC Policy, SOP, Application and Authorisation, as well as the Human Rights Impact Assessment and Data Protection Impact Assessment, 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?

N/A

6. Have you identified any areas where action is required to conform more fully with the requirements of Principle 2?

☐ Yes ☒ No

**Action Plan**

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?

HIOWC already has in place and publishes information regarding where to direct general police complaints as well as data protection specific complaints including publishing contact details for its Data Protection Officer (DPO).

In connection with the LFR Deployments, however, HIOWC 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 Corporate Communications Department who will send any requests or complaints to the appropriate handling departments including:
- Joint Information Management Unit for requests to exercise data subjects rights or Freedom of Information requests.
- Professional Standards any complaints regarding the conduct of officers involved with the LFR deployment.
- LFR Team to respond to requests regarding the process and deployment of LFR.
- Legal Team should there be a legal challenge to the use of LFR.
- Corporate Communications to signpost to additional HIOWC published information about its use of LFR.

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 HIOWC is subject to existing law and regulation, the College of Policing Authorised Professional Practice on Live Facial Recongition and HIOWC's own Policy and SOP as well as remaining HIOWC LFR Documentation.

The LFR deployments will be delivered using specialist equipment operated by the Hampshire & Isle of Wight Constabulary and Thames Valley Police collaborated Joint Operations Unit, LFR Team. During the preparation and delivery of a specific LFR deployment the LFR Team will be acting under the direction and control of the Chief Constable (as data controller) that is requesting the deployment in their force, according to the arrangements set out in their own LFR Policy and Standard Operating Procedure and other associated LFR impact assessments and documents.

Prior to the deployment, consultations have been undertaken with the HIOW Police and Crime Commissioner and other apropriate represenatative groups. This will be ongoing.

In addition to external oversight, HIOWC is committed to internal oversight of the deployments and will therefore gather and assess data at the conclusion of each individual deployment as well as periodcally to assess the efficacy and ongoing justification for and proportionality of the use of LFR. A Gold Commander is appointed in connection with deployments and the HIOWC LFR SOP establishes requirements for the application for and authorisation of LFR deployments, usually by an officer of a rank of no less than Superintendent. A Silver Commander, as a single point of contact, will oversee the tactical delivery of LFR at all LFR deployment sites.

An LFR retention and disposal schedule outlines the retention periods for data collected during the deployment of LFR and specifies the roles that are responsible for ensuring data deletion occurs at the appropriate time.

If the evaluation of the LFR trial demonstrates that there is a justifiable benefit for HIOWC to use LFR in the future, consideration will be given to the most appropriate additional LFR governance structure to be put in place prior to future LFR deployments.

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

As well as a Gold Commander being appointed in connection with the deployment of LFR, as stated above a single point of contact has been established in connection with LFR deployments to supplement existing procedures and this will be publicised online as well as

in the information provided to those who are the subject of an engagement.

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?

HIOWC is responsible for the deployment and is the data controller in respect of the processing of personal data.

All individuals involved in LFR deployments will be briefed on their role and the importance of exercising independent judgement.

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 HIOWC LFR Documentation in so far as is appropriate to their role.

If the evaluation of the LFR trial demonstrates that there is a justifiable benefit for HIOWC to use LFR in the future, a schedule of refresher training will be put in place, e.g. annually.

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?

HIOWC officers and staff will be operating the CCTV system.

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?

HIOWC 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?

N/A

28. If you deploy surveillance cameras using drones, have you obtained either Standard Permission or Non-Standard Permission from the Civil Aviation Authority and what is your CAA SUA Operator ID Number?

☐ Yes ☐ No

N/A

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

☐ Yes ☒ No

**Action Plan**

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 minimum of 31 days, but this period may be extended where necessary for example in the event of a complaint, investigation or prosecution. Biometric templates of those that generate an alert from the watch list will be deleted within 24 hours of the conclusion of the deployment. Biometric templates of those who do not generate alert on the watchlist will be deleted automaticlaly and almost instantaneously. 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.
Other deletions of images are manual and the responsibility of the following persons to delete:
- LFR Operators: CCTV feed, watchlist images from LFR system and match alerts.
- Silver Commander for each deployment: watchlist from encrypted USB (from which the watchlist is uploaded onto the LFR system).
- Strategic LFR Lead: watchlist metadata in CSV file, logs / records of each deployment, and LFR governance documents (using assigned timebased retention labels in the HIOWC content and document management system).

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?

Access to biometric data and CCTV images are privileged. They will be stored in access controlled digital storage. Requests to access any retained images and information will be considered on a case by case basis by a designated central point in the LFR Team to ensure any access is both necessary and proportionate. Some departments are expected to request access in the context of their role in overseeing the LFR Deployments, eg: the Joint Information Management Unit who may need access to specified information to consider a data subject's request to exercise their data rights.

Biometric templates are retained for such short periods of time it is not anticipated that further use would be feasible, however in connection with these images as well as CCTV images, any re-use of such data must be compliant with the Data Protection Act 2018 and/or UK GDPR and Human Rights Act 1998 and wider legal and regulatory obligations.

37. Do you have a written policy on the disclosure of information to any third party? ☒ Yes ☐ No

38. How do your procedures for disclosure of information guard against cyber security risks?

All data held on police systems is subject to review / retention / deletion schedule of the National Police Chief's Council Authorised Professional Practice on Information Management and HIOWC Information Management policies and procedures.

The LFR system is a siloed non-networked system, which is subject to security measures, including: the LFR application has two layers of password protection to access the application; the LFR application is staffed when in use and therefore physical protections are in place; LFR system Operators are deployed with the system when in operation; deployment data stored on the system is securely wiped following each Deployment; individual users of the LFR application and subject to role based access controls with limited user permissions; the Dashboard and RESTful API are secured with SSL and TLS by default, and all connections are directed through HTTPS; the LFR application can be connected to mobile devices using a private access point with three levels of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App; and, logging data is retained of user activity which enables auditing to be conducted.

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

HIOWC has established policies and procedures on handling data subject access requests and individuals will be entitled to make such requests either via the standard published route, direct to the Data Protection Officer and/or to the dedicated LFR point of contact.

Any information held at the date of the request relating to the individual will be considered for disclosure.

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?

HIOWC's Information Management Policy sets out requirements for information sharing. Those departments that are more likely to need to access LFR information after a deployment (eg: Joint Information Management Unit, Professional Standards Department and Legal Team) will record any disclosures within their relevant case management systems.

If LFR information is subsequently included in a prosecution file, its disclosure will be recorded on the HIOWC crime recording / case preparation system.

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 system and CCTV system are both developed by highly accredited companies who are leaders in their field. The systems have been rigorously tested both by the manufacturers and in the case of LFR technology by NIST (National Standards for Institutes and Technology) for accuracy including demographic and gender bias.

HIOWC LFR processes and associated guidance have been developed so as to provide for a reliable means of locating individuals using LFR with high definition CCTV cameras (2MP and above). For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the LFR Operator, and associated policing resources on the ground. A system using facial recognition will consist of many components.

The current LFR system has also undergone commissioned evaluation by the National Physical Laboratory in (Evaluation Repoert 2023: frt-equitability-study_mar2023.pdf (science.police.uk)

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

Assurances are provided by the LFR Team who have received formal training on the set up and use of the LFR system that HIOWC will be using.

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**

| |
|---|
| The LFR Team will retrospectively analyse the efficacy of the LFR system after deployments to ensure that the set up of LFR cameras and systems is optmised in future deployments. |

## 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?

When held on police systems, all data is subject to the National Police Chief Council's Authorised Professional Practice on Information Management and HIOWC's Information Management policies and procedures.

When data is transferred from HIOWC systems to the standalone LFR system, this is conducted via an encrypted USB memory stick which is the responsibility of the Silver Commander and is required to be securely wiped within 24 hours of the deployment.

As stated above, the LFR system itself is a siloed non-networked system, which is subject to security measures, including: the LFR application has two layers of password protection to access the application; the LFR application is staffed when in use and therefore physical protections are in place; LFR system operators are deployed with the system when in operation; deployment data stored on the system is securely wiped following each Deployment; individual users of the LFR application and subject to role based access controls with limited user permissions; the Dashboard and RESTful API are secured with SSL and TLS by default, and all connections are directed through HTTPS; the LFR application can be connected to mobile devices using a private access point with three levels of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App; and, logging data is retained of user activity 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?

As set out above, the LFR System is a siloed non-networked system.

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

In addition to overarching procedures, instructions and/or guidelines such as the National Police Chief's Council Authorised Professional Practice on Information Management, and HIOWC Data Protection policies and procedures, regard is required to be had to the College of Policing APP on Live Facial Recognition, and the HIOWC LFR Documentation including the LFR Policy and 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?

| |
|---|
| 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**

| |
|---|
| 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?

The deployment of LFR by HIOWC will remain under ongoing internal and external review throughout the period of proposed deployments. A LFR governance structure will periodically review the LFR Team's post deployment evaluation of each LFR deployment in order to oversee proportionality and efficacy of LFR use.

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 HIOWC LFR Policy and SOP, as well as the DPIA and other HIOWC 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?

HIOWC has arrangements in place with the supplier of the LFR system to provide technical IT support if required.

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 HIOWC technical teams during the design of a script to extract images, from HIOWC's crime recording system, of persons to be placed on a watch list enables the selection according to specific criteria - as set out in any LFR Application and Authorisation. The effectiveness of the script has been tested for extraction accuracy.

Prior to the 24 hours pre-LFR deployment a test run of the script will occur to ensure that the script is selecting images as per the designated criteria.

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 HIOWC 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 Watchlist image and comparing that template to templates extracted from CCTV images of individuals passing through the LFR zone of recognition.

As set out in the HIOWC 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?

As set out in the HIOWC LFR Policy, SOP and other LFR Documentation, there are specified categories of individual who may be included on a Watchlist, specifically individuals wanted on warrant, individuals wanted on suspicion of the commission of a range of criminal offences including high risk crimes and those relating to local district priorities which justify inclusion, high and medium risk missing persons, and in cirucmstances where there are grounds to believe that those individuals may be in the vicinity of the proposed LFR deployment location. 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 National Police Chiefs Council's Authorised Professional Practice on Information Management and other court decisions. Mechanisms are in place in accordance with the HIOWC Policy and SOP to ensure that only lawfully held images are considered for inclusion in an LFR Watchlist.

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. |