

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	Thames Valley Police
Scope of surveillance camera system	Version 2.0 (review dated 29/07/2026): Mobile CCTV units with integrated Live Facial Recognition (LFR) software captures images of individuals within designated zones of recognition. For the purposes of locating persons of interest, facial features are converted into biometric templates and compared against a watchlist of persons: who are wanted (on warrant, recall to prison, suspected of / likely to commit an offence); to enforce court or police-imposed orders / conditions; who pose a risk of harm or are at risk of harm; missing persons; or a victim / witness to a serious crime. Biometric templates without a match are deleted almost instantly. Original CCTV footage is retained for at least 31 days, or longer if required for evidence or complaint investigations.
Senior Responsible Officer	Craig Kirby

Position within organisation	Detective Chief Superintendent Crime & Criminal Justice
Signature	
Date of sign off	

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?

The TVP Live Facial Recognition (LFR) Policy states that LFR is used by TVP as a precision crime-fighting tactic to locate people who are of interest to the police. It helps us reduce violence and the risk of harm, to prevent and detect crime and to apprehend and prosecute offenders, securing the administration of justice and maintaining public confidence.

Watchlists, and any images of persons of interest for inclusion on a Watchlist, must be limited to the following categories:

- a) Wanted by way of an outstanding warrant for their arrest issued by a court or are sought for recall to prison.
- b) About whom there are reasonable grounds for suspecting that they have committed a criminal offence.
- c) Who are subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment.
- d) Who are currently subject to legally enforceable restrictions or conditions, in order to monitor compliance with those restrictions or conditions, where compliance can be monitored through the individual's presence, conduct or both, within the deployment location. This includes MAPPA subjects (including registered sex offenders) and persons subject to police or court-imposed conditions, such as bail conditions or court orders, where the restrictions or conditions relate to relevant offences.
- e) About whom there is credible intelligence, a known history of relevant and recent offending, or both, that gives rise to reasonable grounds for suspecting that they are likely to commit a serious or hotspot crime, pose a risk to public safety, or cause other harm, including self-harm.
- f) Who are designated as a Missing Person.
- g) About whom there is credible intelligence that gives rise to reasonable grounds for suspecting that they are at real risk of serious harm.
- h) About whom there is credible intelligence that gives rise to reasonable grounds for suspecting that they are likely to be a victim of, or witness to, a serious crime.

In respect of all persons sought, both the seriousness of the suspected offence or other harm, and its prevalence and local impact will be considered.

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

Lawful basis for the processing of personal data is stated as follows:

- Personal data:

- TVP will not rely on an individual's consent to process their personal data for LFR purposes and therefore where processing takes place pursuant to Part 3 Data Protection Act 2018, i.e. for the law enforcement purposes, the processing of personal data takes place in accordance with section 35(2)(b) Data Protection Act 2018, i.e. the processing is necessary for task carried out for the law enforcement purposes by TVP, which is a competent authority for the purposes of the Act;
- the "law enforcement" purpose, defined in section 31 Data Protection Act 2018, is: the prevention, investigation, detection, and prosecution of criminal offences; the execution of criminal penalties; and the safeguarding against and the prevention of threats to public security;
- TVP's processing of personal data for LFR must also be 'authorised by law' which is met by the 'policing purpose' set out in the Statutory Code of Practice on Police Information and Records Management; and
- where processing takes place pursuant to the UK GDPR (e.g. for the location of missing persons, or the evaluation of efficacy and equitability of LFR), the processing meets one or more of the following requirements: 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].

- Special Category / Sensitive data:

- TVP will not rely on an individual's consent to process their sensitive data for LFR purposes and therefore TVP relies on the following conditions from Schedule 8 of the DPA 2018 and has an Appropriate Policy Document in place:
 - o Statutory etc. purposes (Schedule 8(1)): 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);
 - o Administration of justice (Schedule 8(2)): processing is necessary for the administration of justice);
 - o Protecting individual's vital interests (Schedule 8(3)): processing is necessary to protect the vital interests of the data subject or another individual);
 - o Safeguarding of children and of individuals at risk (Schedule 8(4)): processing is necessary to protect individuals, under 18yo or over 18yo and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual);
 - o Personal data already in the public domain (Schedule 8(5)): processing relates to

personal data which has been manifestly made public by the data subject); and

o Legal claims (Schedule 8(6)): processing is necessary for in connection with legal proceedings, obtaining legal advice, or establishing / exercising / defending legal rights).

- TVP will not rely on an individual's consent to process their special category data for LFR purposes and therefore TVP relies on the following conditions from article 9(2) of the UK GDPR and Schedule 1 of the DPA 2018 and has an appropriate policy document in place:

o Article 9(2)(c)): processing 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;

o Article 9(2)(e)): processing relates to personal data which are manifestly made public by the data subject;

o Article 9(2)(g)): processing necessary for reasons of substantial public interest provided for in domestic law. The substantial public interest conditions require a condition from Part 2 of Schedule 1 of the DPA 2018 to be satisfied, as follows:

i. Schedule 1, Part 2(6) Statutory and government purposes: 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.

ii. Schedule 1, Part 2(8) Equality of Opportunity or Treatment: Processing is necessary for the purposes 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.

iii. Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk: processing is necessary to protect individuals, under 18yo or over 18yo, and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

• Criminal data:

- TVP will process criminal offence data during LFR deployments and under Article 10 of the UK GDPR and section 10(5) of DPA 2018 the processing must satisfy a condition from Parts 1-3 of Schedule 1 of the DPA 2018. TVP meets the following conditions:

i. Schedule 1, Part 2(6) Statutory and government purposes: 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.

ii. Schedule 1, Part 2(8) Equality of Opportunity or Treatment: Processing is necessary for the purposes 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.

iii. Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk: processing is necessary to protect individuals, under 18yo or over 18yo, and at risk from neglect or

physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

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

Necessity:

TVP recognises that the use of LFR is novel and can constitute a material interference with an individual's privacy. However, TVP considers that LFR can deliver considerable policing benefits.

The Home Office published a consultation on 4 December 2025 which identified a number of benefits of the use of LFR included locating individuals wanted for serious criminal offences, leading to arrests for criminal offences, assisted with ensuring registered sex offenders were complying with court-imposed sanctions, and locating high-risk missing children.

In relation to missing persons, the nature of these incidents is often such that locating the individual is a priority given the risk they may pose to themselves or others.

Therefore, while alternative, less intrusive measures of locating persons who are: wanted (on warrant, recall to prison, suspected of / likely to commit an offence); to enforce court or police-imposed orders / conditions; who pose a risk of harm or are at risk of harm; missing persons; or a victim / witness to a serious crime; are available TVP considers that option of appropriate use of LFR is more likely to protect the rights of individuals, particular having regard to the fact that those other methods require higher ratios of police officers and staff. Further, as explained herein, a number of safeguards have been adopted to ensure that LFR is used in a proportionate manner.

Proportionality:

The individuals whose images can be included on a Watchlist to locate individuals who are: wanted (on warrant, recall to prison, suspected of / likely to commit an offence); to enforce court or police-imposed orders / conditions; who pose a risk of harm or are at risk of harm; or a victim / witness to a serious crime. In these circumstances, and for these individuals, TVP considers that, having regard to the law enforcement purposes which are strongly engaged, when balanced against the rights of affected individuals and taking into consideration the safeguards which are in place, an interference with individual rights is subject to appropriate safeguards considered to be proportionate to the aim pursued.

In relation to missing persons, the risk that may be posed by those individuals to themselves and/or others, and the need to safeguard them and the general public, when balanced against the interference with individual rights is subject to appropriate safeguards considered to be proportionate, in the round.

The above assessments take into account the processing of the personal data of members of the public who are passing through the Zone of Recognition. The impact on those rights is extremely limited (and has been characterised by the Court of Appeal as "negligible"). The use of LFR requires matching data, and therefore the processing of the personal data of members of the public who pass through the Zone of Recognition is required as part of an LFR Deployment. Taking into account the negligible impact on their rights, the fact that

each LFR Deployment is overt and transparent, that there are safeguards in place, the processing is considered to be proportionate to the pressing social aim pursued.

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

TVP has fully considered it's use of LFR and documented those considerations and intentions in the following set of LFR documents, several of which are published on the TVP LFR webpage:

TVP LFR Legal Mandate

TVP LFR Policy

TVP LFR Standard Operating Procedure (SOP)

TVP LFR Equality Impact Assessment

TVP LFR Human Rights Impact Assessment

TVP LFR Data Protection Impact Assessment

TVP LFR specific Privacy Notice

TVP LFR specific Appropriate Policy Document

TVP LFR deployment specific Application and Authorisation

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, a Data Protection Impact Assessment has been carried out and published.

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?

TVP already publishes a privacy notice which details individual's data protection rights, including providing details of the DPO and rights of recourse. A specific supplementary privacy notice has been prepared and published in relation to TVP's LFR Deployments, providing further detail of the specific application of these rights.

Both of these privacy notices will be available online. They will also be highlighted to individuals at the perimeter of the Zone of Recognition. For those individuals who are engaged with by an LFR Engagement Officer further to a potential Watchlist match being flagged by the LFR system, the LFR Policy and SOP require those individuals to be proactively offered LFR information leaflets that will deliver key messages about how LFR works and signpost to further information on the TVP LFR website about their rights and mechanisms to seek recourse.

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?

Nationally, the 'National Police Chiefs Council Facial Recognition Technology Board' provides oversight for the use of facial recognition within UK Law Enforcement. TVP are members of the Board, which ensures wider understanding and support for national objectives and priorities. TVP has engaged with representatives from the Information Commissioner's Office prior to the first deployment of LFR and engagement will be ongoing, as and when required.

The Chief Constable of TVP will be the data controller for deployments conducted by TVP, for the purpose of TVP's policing objectives in the TVP geographical area.

In support of meeting the public sector equality duty (PSED), and ensuring that LFR Deployments are not discriminatory, TVP has carried out an LFR Equality Impact Assessment (EIA) which shall be reviewed at least annually and kept under periodic monitoring throughout the period during which LFR Deployments are undertaken to ensure that any learning or trends can be identified and addressed at an early stage. That EIA should be read in conjunction with the Data Protection Impact Assessments and the Human Rights Impact Assessment.

The TVP Authorising Officer (AO) rank is set at Superintendent for Authority to deploy LFR. The AO will review the LFR application for each deployment and any associated documents such as the Community Impact Assessment. The AO will ensure that the deployment of LFR is legitimate, necessary and proportionate.

For each LFR deployment a Gold / Silver / Bronze command structure will be in place.

After the deployment the LFR Deployment Record must be submitted for review within 31 days.

Whilst the TVP Police and Crime Commissioner has been consulted regarding the deployment of LFR in principle, the AO will notify the TVP Police and Crime Commissioner (or designated staff member) prior to any specific deployment.

TVP's independent advisory groups (IAGs) are an independent source of advice. The 'Chairs of IAGs Group' has been consulted prior to the initial first use of LFR by TVP and will continue to be engaged as required.

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 TVP Strategic Lead for LFR is the Detective / Chief Superintendent for Crime and Intelligence who is also the TVP Gold Commander for LFR and the joint chair for the TVP and Hampshire and Isle of White Strategic Facial Recognition Board.

-
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?

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

LFR deployments will run by a dedicated and trained LFR Team who will brief additional officers supporting the deployment prior to its commencement. The briefing will emphasise the importance of using their own professional judgement..

There will be a clear Gold / Silver / Bronze command structure in place for each LFR 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 deployment will receive training in advance as well as a briefing on the day of the deployment. The LFR system operators have had specific technical training on how to operate the LFR system and cameras. This ensures that individuals fully understand how the LFR system works, its limitations / sensitivities, and the TVP LFR documentation that is relevant to the role they play in the deployment.

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?

The occupational standards for this role are considered to be comparable to other occupational standards within the TVP.

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?

TVP 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?

NPCC Body Worn Video Guidance:

<https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/local-policing-coordination-committee/2024/npcc-bwv-guidance-2024.pdf>

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?

TVP has a retention schedule for the retention and deletion of data processed for the purposes of deploying LFR and it can be found in the published LFR Appropriate Policy Document on the TVP LFR webpage.

Where the LFR system does not generate an alert, a person's biometric data derived from the live LFR CCTV feed is immediately automatically deleted. Where the LFR system does generate an alert, that person's biometric data derived from the live LFR CCTV feed is deleted within 24 hours following the conclusion of the deployment.

Watchlist data held on an encrypted USB memory stick used to import the watchlist onto the LFR system is deleted within 24 hours following the conclusion of the deployment.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- due to its relevance in a criminal investigation and is then held in accordance with the Data Protection Act 2018, UK GDPR, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- in accordance with TVP's complaints / conduct investigation policies or other legal obligations.

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

Where the LFR system does not generate an alert a person's biometric data derived from the live LFR CCTV feed is immediately automatically deleted. Where the LFR system does generate an alert, that person's biometric data derived from the live LFR CCTV feed is deleted within 24 hours following the conclusion of the deployment.

TVP has a retention schedule for the non-automatic deletion of data processed for the purposes of deploying LFR and can be found in the published LFR Appropriate Policy Document on the TVP LFR webpage.

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 Control:

Biometric data and CCTV images are classified as privileged information and stored in secure, access-controlled digital systems.

- Access Requests:

Any request to access retained images or associated information will be assessed on a case-by-case basis by a designated central point within the LFR Team to ensure necessity and proportionality. Certain departments, such as the Joint Information Management Unit, may require access for specific purposes, including responding to data subject rights requests.

- Retention and Re-use:

Biometric templates are retained for very short periods, making further use unlikely. However, any re-use of biometric or CCTV data must comply with the Data Protection Act 2018, UK GDPR, Human Rights Act 1998, and all other applicable 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?

Procedures and process to prevent cyber security risks are reviewed by the Joint Information Management Unit. There are strict processes that need to be followed to prevent this risk. Our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. The security of the LFR system has been assessed by the TVP ICT department.

The LFR system is non-networked and non-configured to extend to the cellular network as an additional geographical protection and is 'closed' and not connected to other TVP systems or the internet.

The watchlist will be downloaded to an encrypted data stick. The data stick will be subject to a physical security process that will ensure it is stored securely and when it is not stored it will be in the physical possession of a police officer. When the deployment has finalised the data stick will be securely deleted or destroyed once the required retention period has passed.

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

TVP already publishes a privacy notice which details individuals' data protection rights, including providing details of the DPO and rights of recourse. A specific supplementary privacy notice has been prepared and published in relation to TVP's LFR Deployments, providing further detail of the specific application of these rights. TVP has a specialist team in their Joint Information Management Unit that responds to data subjects who choose to exercise their data rights.

<https://www.thamesvalley.police.uk/rqp/request/ri/request-information/>

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?

TVP will not routinely share LFR personal data except where we are required to do so when working with other police forces, law enforcement bodies, and / or other agencies to assist TVP in discharging its common law policing powers. This action will not involve the sharing of biometric data but may involve sharing personal data.

TVP has an Information Management Policy, intranet information sharing guidance, Joint Information Management Unit and Data Protection Officer to provide expert advice, when needed, on a request to share LFR data further however; the personal data used specifically for LFR or collected during LFR deployments will be deleted within 31 days after the end of the deployment unless needed as evidence or to investigate an investigation into police officer conduct.

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 have been rigorously tested both by the manufacturers and in the case of LFR technology by NIST (National Standards for Institutes and Technology).

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

The specific technology to be used in the TVP LFR Deployments has been subject to scientific testing both as to its efficacy and the potential for bias and discrimination. The National Physical Laboratory's scientific testing found that at a setting of 0.64 (algorithm threshold) there was equitability of facial matching accuracy across all demographics. In TVP's consideration of the threshold setting it will adopt, it has reviewed the LFR deployments made by South Wales Police where (at the time of writing this document) no inaccurate matches were experienced at a threshold setting of 0.64. TVP will deploy LFR with an accuracy setting of 0.64 and carry out its own equitability evaluation after each deployment.

Assurances are provided by the LFR Team who have received formal training on the set up and use of the LFR system that TVP 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 TVP LFR Team will analyse and evaluate the efficacy and equitability of the LFR system after each deployment. This analysis will be reported periodically to the Joint TVP and Hampshire & Isle of Wight Strategic Facial Recognition Board.

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?

The LFR System has been assessed by the TVP ICT department. The LFR system is subject to the following security measures:

Technical:

- The application is non-networked and non-configured to extend to the cellular network as an additional geographical protection.
- The LFR application is 'closed' and not connected to other TVP systems or the internet.
- The TVP watchlist is transferred from the TVP crime recording system by encrypted USB to the closed LFR System where it is uploaded.
- The Dashboard and RESTful API are secured with SSL and TLS by default.
- All connections are directed through HTTPS.

Organisational:

- Two types of access will be available to the application – 'user' and 'administrator' access levels.
- Passwords are security protected.
- LFR System operating staff will have police vetting clearance.
- Role- based access controls.
- LFR System access is only granted to users following completion of training.
- The LFR system is staffed when in use and therefore physical protections are in place.
- The physical encrypted USB remains the responsibility of a specified member of the LFR Team during the LFR deployment.

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 LFR system is a non-networked, stand-alone 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?

The TVP LFR SOP and LFR system security instructions inform the TVP LFR Team on the necessary security measures that they need to implement.

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. Body Worn Video used at LFR deployments is part of standard police procedure and it is not an intrinsic part of LFR deployments.

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 at this time.

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 TVP LFR SOP requires that any authority given by the Authorising Officer to deploy LFR:

- a) Must articulate the legitimate aim of the Deployment and the legal powers that are being relied upon to support the Deployment; and
- b) means that the AO is satisfied that the Deployment complies with TVP LFR documents, or is otherwise authorised; and
- c) must, from a Human Rights Act 1998 perspective, articulate
 - i. how and why the Deployment is necessary (and not just desirable),
 - ii. is proportionate to achieve the legitimate aim of the Deployment; and
 - iii. that any interference with individuals human rights has been carefully considered and believed to be proportionate means of achieving the legitimate aim of the deployment;

The TVP LFR Team will analyse and evaluate the efficacy and equitability of the LFR system after each deployment. This analysis will be reported periodically to the Joint TVP and Hampshire & Isle of Wight Strategic Facial Recognition Board. The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (including what methods were used to obtain them):

- a) total number of individuals and the total number of images included in the Watchlist (there may be multiple images of some individuals); and
- b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR system was able to generate a Template from them); and
- c) total number of Alerts that do not result in an Engagement; and
- d) total number of Alerts where a decision was taken to Engage an individual; and
- e) total number of Alerts that are confirmed as correct (the individual is who the LFR system suggests are); and
- f) total number of correct Alerts that result in an Engagement that do not require any further police action; and
- g) outcome of each case where police action is instigated following an Alert; and
- h) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome.

After each LFR deployment, the LFR Team will publish non-personalised results on the TVP LFR webpage.

The TVP LFR document set will be kept under regular review.

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

None at this time ahead of initial TVP LFR deployments..

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

Staff have received additional technical / maintenance training to ensure the operational effectiveness of both LFR vans. TVP 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?
- There has been engagement with TVP ICT Team in the development of the script that extracts the images of persons meeting the criteria to be included on the watchlist for that deployment, from the TVP Crime Recording System. The effectiveness of the script has been tested for extraction accuracy.

A bespoke Community Impact Assessment will be completed for most deployments.
-
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?

This self-assessment is for Live Facial Recognition deployments only.

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

The TVP LFR Policy and TVP LFR SOP state the categories of persons that could be included on the watchlist, as stated in principle 1, question 1 of this assessment.

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 TVP LFR Retention Schedule within the TVP LFR specific Appropriate Policy Document outlines the retention periods for LFR data and is published on the TVP LFR webpage.

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.