Thames Valley Police Policy Document for the Overt Deployment of Live Facial Recognition Technology

---

1. INTRODUCTION, AIM AND SCOPE

Introduction

1.1. Live Facial Recognition (**LFR**) assists Thames Valley Police (**TVP**) as a precision crime-fighting tactic to locate people who are of interest to the police. More detail about how LFR works and how TVP use it can be found in section 4 (LFR Overview).

1.2. This LFR Guidance Document provides TVP personnel with advice on the overt use of LFR in a legally complaint and ethical manner to enable TVP to achieve legitimate policing aims.

1.3. 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. 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.

1.4. In completing this document TVP has taken into account the views and considerations of the Information Commissioner, Biometrics and Surveillance Camera Commissioner, the courts, national guidance and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (**LEA**). This document will be periodically reviewed and updated to reflect material developments in those views and considerations.

Aim and Scope

1.5. This guidance aims to: -

1.5.1. provide TVP personnel and members of the public with information about TVP's present strategic, operational and technology objectives for the overt use of LFR, such that it enables TVP to achieve its law enforcement purposes; and

1.5.2. provide TVP personnel with guidance on the deployment of overt LFR technology by TVP in spaces accessible to the public to meet TVP's objectives for LFR; and

1.5.3. establish the governance structure for the deployment of LFR, ensuring that TVP use of LFR is appropriately governed and legally compliant; and

1.5.4. provide an overview of LFR technology and advise on practical issues such as camera selection and placement to obtain the best performance from the LFR system.

Not in Scope

1.6. There are other forms of facial recognition technology (**FRT**) that are not subject of this guidance. This includes Retrospective Facial Recognition, which relates to non-real time searching of images against a database. Also, not in scope is Operator Initiated Facial Recognition where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis and most importantly not in a 'live' function.

1.7. In summary, this guidance does not extend to: -

1.7.1. manually instigated facial recognition for retrospective searching of video / still images;

1.7.2. human initiated facial search submitted from a mobile device in near real-time;

1.7.3. any TVP use of third-party LFR systems used for a commercial purpose (e.g. 'Facewatch'), or data sharing for the purpose of facilitating the use of those systems. In such instances additional privacy considerations would be required (e.g. additional Information Sharing Agreements and audit requirements), which are beyond the scope of this guidance; or

1.7.4. the legal framework applicable to TVP's use of LFR – this is separately detailed in TVP's Legal Mandate document.

Additional Documents

1.8. A number of documents are available to supplement this guidance, and these include but are not limited to: -

1.8.1. TVP LFR Standard Operating Procedure (**SOP**)

1.8.2. TVP LFR Data Protection Impact Assessment (**DPIA**)

1.8.3. TVP LFR Legal Mandate

1.8.4. TVP LFR Appropriate Policy Document

1.8.5. TVP LFR Human Rights Impact Assessment

1.8.6. TVP LFR Equality Impact Assessment

1.8.7. TVP LFR Community Impact Assessment

1.8.8. TVP Surveillance Camera Code Self-Assessment

1.8.9. TVP LFR Privacy Notice

1.9. In addition, in relation to any deployment(s), there will be an LFR Application, LFR Authorisation, a watchlist, the TVP LFR Deployment Logs and Cancellation Report.

2. LEGISLATIVE COMPLIANCE

2.1. This document has been drafted to comply with the principles of the Human Rights Act 1998, Data Protection Act 2018, UK GDPR and Equality Act 2010. It pays particular attention to the duties of the force regarding privacy, protection from discrimination and the rights to assembly, thought and expression. It should be read in conjunction with the remaining TVP LFR Documentation.

2.2. Equality and Diversity duties and issues have been considered and this is reflected in the Equality Impact Assessment and Human Rights Impact Assessment that is provided alongside this document.

2.3. As with all policies, the duties, and obligations of the force regarding Data Protection, Freedom of Information, Human Rights and Equalities Matters have been considered and complied with, along with The College of Policing's Authorised Professional Practice (**APP**) on Facial Recognition Technology.

3. TERMINOLOGY

3.1. Within TVP and throughout TVP's LFR Documentation, the following terms and definitions apply in relation to Live Facial Recognition:

Adjudication

A human assessment of an alert generated by the Live Facial Recognition application by an LFR engagement officer (supported, as needed by the LFR

operator) to engage and further confirm identification with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject, system and environmental factors.

Alerts

An alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the watchlist and returns a comparison (similarity) score above the threshold.

True Alert

A true alert is determined when the biometric template from the probe image is the same as the biometric template of the candidate image in the watchlist.

Confirmed True Alert

Following engagement, a confirmed true alert is determined when the engaged individual is the same as the person in the candidate image in the watchlist.

True Recognition Rate

It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated). This is also referred to as the true positive identification rate.

False Alert

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement.

(The false alert rate is one of the two measures relevant to determining application accuracy).

Confirmed False Alert

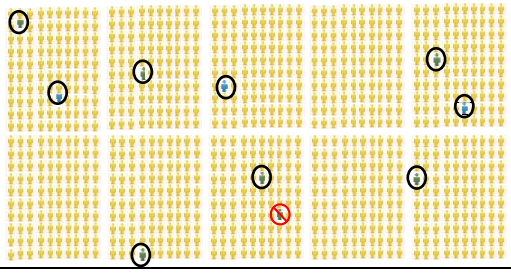
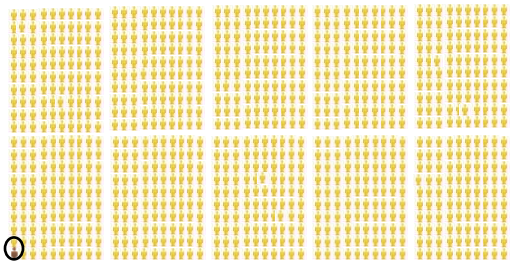
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

False Alert Rate

The number of individuals that are not on the watchlist who generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition. This is also referred to as false positive identification rate.

Application Accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the ‘True Recognition Rate’ and the ‘False Alert Rate’. This is further explained below. The example given has been simplified to demonstrate the concept, but note that the metrics have been calculated in accordance with the agreed scientific method as set out by the International Organisation for Standardisation:

		True Recognition Rate	False Alert Rate
What is it?		It is the total number of times an individual(s) on a watchlist is known to have passed through the Zone of Recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the Zone of Recognition. This is regardless of whether an alert is generated by the LFR application or not.	Is the number of individuals that are not on the watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
Worked Example		The True Recognition Rate would be 90% if 10 people on the watchlist each pass the LFR system, and an alert is generated correctly for 9 out of 10 of those people (with no alert being generated against the 10th person). 	The False Alert Rate would be 0.1%, if for every 1,000 people that passed the LFR system, an alert was generated against one person who was not on the watchlist. 

Authorising Officer (AO)

The officer (holding the rank of Superintendent or above) who provides the authority for deployment of LFR.

Biometric Template

A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

Blue Watchlist

A blue watchlist comprises known persons that can be used to test system performance, for example, police officers / staff may be placed on a blue watchlist and `seeded' into the crowd who walk through the zone of recognition during a deployment.

Candidate Image

Image of a person from the watchlist returned because of an alert.

Deployment
Use of an LFR application as authorised by an AO to locate those on an LFR watchlist at a designated location.

Deployment record
An amalgam of the LFR Application, the Written Authority Document and the LFR Cancellation Report. This sets out the details of a proposed deployment including – but not limited to:

a. location
b. dates and times
c. deployment and watchlist rationale
d. legal basis
e. necessity
f. proportionality
g. safeguards
h. watchlist composition
i. authorising officer
j. resources
k. relevant statistics
l. outcomes
m. summary of any issues
n. threshold setting

Engagement
An officer communicating with a member of the public as a result of an alert and the ultimate decision maker in respect of any appropriate action that is or is not taken by police in respect of that person.

Environmental Factors
An external element that affects LFR application performance, such as dim lighting, glare, rain, mist.

Faces per frame
A configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.

Facial Recognition Technology (FRT)
This technology works by analysing key facial features, generating a mathematical representation of these features (the Biometric Template), and then comparing them against the mathematical representation of known faces in a database and generates possible matches. This is based on digital images (either still or from live camera feeds).

False Negative
Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are several reasons false negatives occur; these include application, subject and environmental factors, and how high the threshold is set.

Gold Commander
Is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment. They are responsible and accountable for the policing operation/event and determine the strategic objectives.

Law Enforcement Agency (LEA)
UK agencies that have powers, based in law, to carry out law enforcement functions e.g: police forces.

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

LFR Engagement Officer
An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR deployment.

LFR Operator
An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

Person(s) of Interest
A person on a watchlist

Possible Match
A person returned because of the probe and candidate image being of sufficient similarity above the threshold.

Probe Image
A facial image which is searched against a watchlist.

Recognition Time
The average time from when a face appears in the zone of recognition of the camera to when the LFR application generates an alert.

Retrospective Facial Recognition (RFR)
A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database to identify them.

Silver Commander
The officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander. The silver commander develops, commands, and coordinates the overall tactical response of an operation, in accordance with the strategic objectives set by the Gold Commander.

Similarity Score
Is a numerical value indicating the extent of similarity between the probe and candidate image, with a higher score indicating greater points of similarity.

Subject Factor
A factor linked to the individual, for example, demographic factors or physical features or behaviours for example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.

System Factor
A factor relating to the LFR application such as the algorithm.

Threshold
The configurable point at which two images being compared will result in an alert. The threshold needs to be set with care to maximise the probability of returning true alerts whilst keeping the false alert rate to an acceptable level.

Urgency
In the context of authorising an LFR deployment, a deployment that is related to an: imminent threat-to-life or serious harm situation; and/or intelligence / investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action.

Watchlist
A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (from the reference image database) and will have been created specifically for the Deployment.

Zone of Recognition
A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.

4. LFR OVERVIEW

LFR in a Law Enforcement Context

4.1. Live Facial Recognition (**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.

4.2. LFR helps locate those on a watchlist, by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a watchlist of Candidate Images of people who are of interest to the police. Watchlist composition is restricted to individuals considered likely to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR deployment. Watchlist composition is also restricted to those linked to the identified purposes of the LFR deployment.

4.3. LFR works by analysing key facial features to generate a mathematical representation of them, the Biometric Template. This representation is then compared against known faces in a database to identify Possible Matches against persons of interest to LEAs. Where the LFR application identifies a Possible Match, the LFR system flags an Alert to a trained member of TVP personnel who then decides whether any further action is required. In this way, the LFR application works to assist TVP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

LFR and Other Forces

4.4. LFR has been trialled by Hampshire & Isle of Wight Constabulary and is now used by a number of other forces, including South Wales Police, Essex, and the Metropolitan Police. TVP believes that LFR is a valuable precision policing tool that may be less intrusive than certain alternatives and will help TVP to keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

4.5. Currently, the only circumstances in which TVP would deploy LFR to locate persons of interest are set out below. This may change as TVP's approach to LFR evolves, in which case this policy and related documentation would be reviewed and updated accordingly.

(a) For the purpose of locating persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison.

(b) Where there are reasonable grounds to suspect the individual of having committed a criminal offence. Both the seriousness of the

suspected criminal offence and the prevalence and local impact of the criminal offence will be considered.

(c) 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) For the purpose of locating individuals who are designated as a current High Risk Missing Person (HRMP). The use of the Missing Person category will be an exception. A High Risk Missing Person is where the risk of harm to the subject is assessed as both likely and serious.

4.6. The inclusion of any category will be determined for each operation, commensurate with the intelligence case and identified threat and risk posed.

4.7. Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK LEA and the public in turn, it is important to recognise that the use of LFR involves biometric processing. TVP is conscious that the use of LFR has been the subject of much debate. Areas subject to particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR (particularly in the context of early deployments by other forces), the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.

4.8. It is therefore incumbent on TVP to ensure that LFR is used lawfully, fairly and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR.

4.9. In seeking to address other potential concerns, law enforcement colleagues have facilitated academic research led by the National Physics Laboratory on the use of LFR technology in an operational context to further build on the high levels of diligence already conducted on the FRT algorithm. TVP have considered this research, consulted with the NPCC and consulted with other forces, all of which has informed the TVP LFR Documentation, and it is available on its website.

4.10. TVP engaged with many parties with an interest in the use of LFR and has carefully considered their constructive views and recommendation in identifying the following safeguards considered to be necessary to support the use of LFR:

4.10.1. Each deployment must be carefully designed and have clear, documented objectives.

4.10.2. The watchlist for any deployment will be restricted to individuals described above, linked to the purpose of the deployment and where there is considered to be a likelihood of individuals from those watchlists being in the vicinity of that deployment.

4.10.3. The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality.

4.10.4. Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any impact on the human rights of the public.

4.10.5. Additional safeguards include: transparency, training, consultation, data retention and destruction and the quality and source of input images.

4.11. The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the deployment are appropriately trained (in the case of operators), briefed, and accountable. Also, that equipment will be used correctly, and that those involved in the deployment mitigate against inappropriate responses to LFR application Alerts.

4.12. The AO must also consider how the deployment of LFR may impact on communities, and how the rights of everyone whose image is likely to be captured by the LFR application have been considered, and what safeguards are in place to protect them.

4.13. TVP is not only concerned with developing and implementing precision policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. TVP will implement a robust governance process to review the effectiveness and impact of its LFR deployment.

4.14. TVP will focus on delivering transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from TVP communities as part of an ongoing process.

4.15. This guidance document will continue to evolve to reflect changes in legislation, regulation, technology, the views of the Information Commissioner, Biometrics and Surveillance Camera Commissioner, the courts, national guidance and accepted use (including by the LEA).

5. STRATEGIC INTENTION, OBJECTIVES AND USE CASE

5.1. LFR Deployments must be run under a Written Authority Document that complies with the following strategic intentions and operational objectives.

Strategic Intentions

5.2. TVP will:

5.2.1. Use overt LFR technology in a responsible and proportionate way to locate persons of interest to the police in accordance with TVP's common law policing powers.

5.2.2. Strengthen and develop LFR technology capability to protect the public, reduce crime, and to help safeguard the public.

5.2.3. Build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns and maximising transparency;

5.2.4. Maintain good governance through a command structure that incorporates strategic, operational, and technical leads for the deployment of LFR, with clear decision making and accountability;

5.2.5. Ensure that the deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Courts, the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and TVP LFR Documentation.

5.2.6. Transparently identify, manage, and mitigate reputational and organisational risk to TVP.

Operational Objectives

5.3. TVP will:

5.3.1. Adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight will be active and involved, with the engagement officer retaining full control in making the decision on whether to take action.

5.3.2. Engage with and provide reassurance to communities, listening and responding to concerns,

5.3.3. Continually identify and review risks relevant to the use of LFR technology and seek to mitigate those risks.

Technological Objectives

5.4. TVP will:

5.4.1. ensure insofar as reasonably possible that all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and

5.4.2. provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic; and

5.4.3. consider technological improvements whilst keeping the TVP LFR SOP under review. Where appropriate we will trial alternative providers of facial recognition software and hardware with a view to ensuring the best possible service and proactively developing improved working methodologies and accuracy. The outcomes of any trials will be captured with the same key performance metrics

that are gathered when deploying LFR to ensure the findings are suitable for direct comparison and analysis. All previously detailed retention periods will remain unaffected. Any trial will have relevant documentation and considerations completed prior to commencement and at the end of the trial.

Use of LFR

5.5. This guidance relates to the use of LFR in an overt capacity to help TVP protect the public. TVP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool.

5.6. Locations for the deployment of LFR will be kept under strict review, with LFR being deployed into areas where it has the greatest potential to assist TVP in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why a location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other TVP LFR Documentation. These principles reflect the College of Police's Authorised Professional Practice guidance on LFR. In general, it is likely to be less justifiable to deploy LFR at particular locations to search for individuals, simply on the basis that a large volume of people frequent or pass through the area. Some locations, such as schools, polling stations, and assemblies, raise greater expectations of privacy; these considerations will be taken into account in assessing locations for deployment.

5.7. Given that LFR requires a member of TVP personnel to review every Alert in real-time for a decision as to whether any further action is required, TVP will ensure that sufficient resources are available to respond to Alerts (having regards to the expected volume of people passing past the LFR) which allows TVP to act on any Alerts as they are generated and will deploy LFR in a way that is operationally effective.

5.8. Operations which make use of LFR will be "time bound" in that the police surveillance conduct using the technology will have clear start and end times and dates.

6. OVERVIEW OF LFR DEPLOYMENT PROCESSES

End-to-End Process

6.1. The end-to-end process of an LFR Deployment can be summarised as follows:

6.1.1. LFR law enforcement purpose identified, safeguards considered, deployment authorised, and watchlist selected in the 24 hours prior to deployment time;

6.1.2. Biometric Templates automatically extracted by the LFR software from images of individuals included in watchlist;

6.1.3. Notification of deployment, and signage deployed;

6.1.4. As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a watchlist;

6.1.5. If a Possible Match is found in a watchlist, the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the watchlist are presented to the LFR Operator / LFR Engagement Officer for human review;

6.1.6. The LFR Operator / LFR Engagement Officer will consider the Alert, (including the image comparison and confidence score), noting the System, Subject and Environmental Factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is Engaged;

6.1.7. Cancellation of authority for the LFR Deployment and post-Deployment evaluation.

6.1.8. Mechanism in place to direct persons wishing to access more information about TVP's use of LFR, exercise their data protection rights or complain to the appropriate responder.

6.2. TVP LFR SOP provides a greater level of detail about the processes involved in the deployment of LFR by TVP. A flowchart summarising LFR Deployment can be found in the TVP Standard Operating Procedure.

Key Points

6.3. LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are on a watchlist;

6.4. The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area;

6.5. The quality and resolution of images (both those in the watchlist and those from the video cameras) are of vital importance and must be carefully considered;

6.6. The inclusion of persons on a watchlist needs to be justified based on the principles of necessity and proportionality; and,

6.7. It is important to balance the objectives of the operation with the size of the watchlist and the available resource to respond to Alerts. If the objectives are too broad and/or the watchlist is too large, the amount of resource required to respond to Alerts may be prohibitively high.

Policing LFR Deployments Effectively

6.8. There must be sufficient appropriately trained resource deployed to be able to respond to Alerts. This is important to ensure that the LFR application, and the data processed by it, is being effectively used.

6.9. The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, Recognition Time, and the probability of people from the watchlist being observed by the camera (i.e. occlusion) and their likely presence; these are all matters that must be considered when deciding what resources should be available for the deployment.

6.10. It is also vital that TVP is transparent in its use of LFR under this guidance. As well as using signage, the provision of sufficient policing resource will allow officers to answer questions that the public may have.

6.11. This will be discharged by:

6.11.1. Having printed LFR information leaflets at deployments for TVP Engagement Officers to provide to any persons they have spoken to as a result of a confirmed LFR match, and any persons in and around the recognition zone;

6.11.2. QR codes and links on LFR leaflets and posters directing individuals to additional LFR information on TVP's website;

6.11.3. Publication of the following LFR documents on the TVP force website (Policy, Standard Operating Procedure, Equality Impact Assessment, Community Impact Assessment, Human Rights Impact Assessment, Legal Mandate, Privacy Notice, Appropriate Policy Document, Data Protection Impact Assessment, Surveillance Camera Code Self-Assessment, Results of previous LFR deployments and FAQs (redacted as necessary);

6.11.4. Details of deployments will be published on the TVP website and social media channels ahead of deployments (7 days prior to deployment);

6.11.5. TVP Engagement Officers will answer questions asked by individuals around the deployment area and be able to direct individuals to further information;

6.11.6. Mechanism for individuals to contact TVP for further information or complain, as above.

7. GOVERNANCE, OVERSIGHT, AND IMPACT ASSESSMENTS

7.1. Following consultation, the following stipulations have been proposed and accepted by TVP:

7.1.1. The overall benefits to the public must be balanced with public confidence of our use of LFR;

7.1.2. Evidence that because of the accuracy threshold used by TVP and associated processes, the technology itself will not result in gender or racial or age accuracy variance resulting in unlawful bias or discrimination in policing operations;

7.1.3. Each deployment must be appropriately assessed and authorised, demonstrating both necessity and proportionality with respect to policing purpose identified for the deployment;

7.1.4. LFR Operators will be accountable for their actions and are trained to understand the risks associated with use of the LFR application, including how potential injustices may be caused through inappropriate responses;

7.1.5. TVP will develop and maintain robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency and the Statutory Biometric and Surveillance Camera Commissioner's Code of Practice, as well as guidance issued by the Information Commissioner and the Courts. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime. This will include Independent Advisory Group panels and ethics committees.

Governance Framework

7.2. TVP LFR documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:

7.2.1. Pre-Deployment;

7.2.2. Operational Deployment;

7.2.3. Post-Deployment.

Pre-Deployment

7.3. TVP Authorising Officer (AO) rank is set at Superintendent for Authority to deploy LFR. The AO will review the LFR application and any associated documents such as the Community Impact Assessment.

7.4. TVP will designate a Senior Responsible Officer as having overall responsibility for the deployment of LFR.

7.5. 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.

7.6. 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.

7.7. Several specific TVP documents and records must be completed in support of each deployment. These are set out below:-

TVP LFR Deployment Specific Documents and Records	
LFR Application	Sets out the details of a proposed deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, watchlist composition, and resources.
Written Authority Document	The AO's written authority provides a decision-making audit trail demonstrating how the AO has considered the legality, strict necessity and proportionality of the deployment of LFR, the safeguards that apply and the alternatives that were considered but deemed to be less viable to realise the policing purpose. The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained because of the LFR Deployment. The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.
Operational Risk Assessment	A documented assessment of specific operational risks associated with a LFR deployment, including decisions taken regarding mitigation
LFR Cancellation Report	Records details of where and when a deployment was carried out, what resources were used, relevant statistics (performance metrics), outcomes and summary of any issues.

Assessments	These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Surveillance Camera Code Self-Assessment. These documents need to be considered by the decision-maker (the AO) when authorising a deployment to ensure they are sufficient to address the issues arising from the proposed deployment. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the deployment is not only necessary, but also proportionate to the policing purpose.
Deployment Logs	Logs completed in the planning and execution of an LFR deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.

7.8. Several other specific TVP documents pertaining to each TVP LFR Deployment have been completed centrally. These are set out below:

TVP LFR Documents and Records	
TVP Data Processing – Appropriate Policy Documents, Privacy Notice and	TVP policy on the processing of data pursuant to the Data Protection Act 2018 and UK General Data Protection Regulation relating to LFR. Transparency tool to inform individuals how their data may be processed by the use of LFR.
Data Protection Impact Assessment, Human Rights Assessment	TVP assessments on how the LFR system and its use complies with: Data Protection Act 2018, UK General Data Protection Regulation, Human Rights Act 1998 and the Public Sector Equality Duty (Equality Act 2010).
TVP Legal Mandate	Outlines the legal considerations to be addressed in order to use LFR.
TVP	Provides the necessary training to ensure those involved in authorising and deploying LFR are familiar and implement the considerations relevant to its lawful, ethical and appropriate use.

Operational Deployment

7.9. Arrangements must be made to accurately record and log the dates, times, and location of the deployment.

7.10. The Silver Commander must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the deployment. The Silver Commander needs to be satisfied that the:

7.10.1. Use of the LFR remains strictly necessary and proportionate for the policing purposes identified in the Written Authority Document; and

7.10.2. Safeguards identified in the Written Authority Document remain effective; and

7.10.3. Level of officer support committed to the deployment is enabling Alerts to be responded to effectively; and

7.10.4. Subject, System and Environmental Factors are such that the use of the LFR application remains effective for realising the policing purpose identified in the written approval.

7.11. Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples include occlusion resulting in those sought not being presented to the camera in cases of high crowd flow, adverse weather / lighting conditions or operational events changing the resources needed in the area. The Silver Commander must be aware of and be able to exercise at their absolute discretion the power to suspend or terminate the deployment. Further details are provided within the LFR SOP.

7.12. The Silver Commander must conduct and record a review of the activity at suitable intervals during the deployment. The timing and frequency of reviews must be determined by the Silver Commander prior to and having regards to the context of the deployment (with a discretion to alter the frequency in response to developments during the deployment). This review should address the continued legality, necessity, and proportionality of the deployment, as well as providing (if appropriate) some analysis on LFR application performance and any engagements undertaken.

Post-Deployment

7.13. The use of LFR should be subject to debrief and review. This will help ensure that future deployments reflect learning identified from each deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the deployment.

7.14. Each deployment should be subject of a Cancellation Report, once concluded.

7.15. The LFR Deployment Record must be submitted to the AO (this may be the same person as the Silver Commander) to ensure that appropriately senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

7.16. The outcome of LFR deployments should be subject to evaluation, which in turn should feed into oversight and scrutiny processes.

7.17. Post-Deployment, TVP must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with TVP LFR documents. This includes that:-

7.17.1. 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;

7.17.2. 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.

7.17.3. the 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.

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

7.18.1. 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

7.18.2. in accordance with TVP's complaints / conduct investigation policies or other legal obligations.

8. BODIES AND REGULATORY FRAMEWORK

8.1. The TVP PCC's office provides a role in the general oversight and scrutiny of policing in TVP.

8.2. TVP LFR Legal Mandate sets out the legal framework for TVP use of LFR technology, whilst TVP LFR Policy Document and TVP LFR SOP support implementation.

8.3. Nationally, the 'NPCC 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.

8.4. Further oversight opportunities may arise in relation to the 'Joint National Biometric Strategic Board'. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the

Information Commissioners Office, and the Biometrics and Surveillance Camera Commissioner. More detail on these roles:-

8.4.1. Biometrics and Surveillance Camera Commissioner; The role of the Biometrics and Surveillance Camera Commissioner is to encourage compliance with the Surveillance Camera Code of Practice, review how the code is working, provide advice to ministers on whether the code requires amendment, and to keep the police use and retention of biometric data under review, including making decisions on applications made by the police to retain DNA profiles and fingerprints, and reviewing national security determinations that are made or renewed by the Police in connection with the retention of DNA profiles and fingerprints. The Commissioner also reports to the Home Secretary about the carrying out of their functions.

8.4.2. Any TVP LFR system will need to comply with the Surveillance Camera Code and the twelve guiding principles. This guidance document, and the remaining LFR Documentation, seeks to apply those principles. See https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.

8.4.3. Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

8.4.4. Section 64 of the DPA 2018 mandates the completion of a DPIA for organisations processing data under Part 3 where this processing is likely to result in a high risk to the rights and freedoms of data subjects. The DPIA must be shared with the ICO if TVP assesses that the use of LFR poses any high privacy / compliance risks that cannot be mitigated.

8.4.5. 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.

9. PUBLIC ENGAGEMENT

9.1. Public engagement must be supported using online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of deployments. At and around the location of deployments, notices and leaflets providing information, including details of the Privacy Notice, should be distributed and feedback via email should be sought.

9.2. Operational briefings delivered to officers and stakeholders prior to deployments should promote openness with the public and transparency about the use of LFR. Officers should be encouraged to engage with the public to increase awareness of how LFR helps keep the public safe and

how it helps bring offenders to justice. Officers will be in possession of information leaflets that can be handed out to the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding, along with signposting to information about redress routes and data subject rights.

9.3. Key stakeholders may be invited to observe the planning and deployment of LFR although it must be noted that the deployment is an operational matter.

In Advance of Deployments

9.4. In advance of deployments TVP will ensure that:

9.4.1. LFR deployments are notified to the public using the TVP website and other appropriate communication channels (including social media); and

9.4.2. LFR awareness raising measures (e.g. signs and leaflets) are prepared to support LFR deployment in line with TVP LFR SOP; and

9.4.3. Literature is prepared for persons who may be engaged (to include information outlined within a privacy notice); and

9.4.4. Officers are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a constable in uniform to compel a person to remove anything that conceals their identity; and

9.4.5. External engagement is considered in discussion with TVP LFR team. It may be appropriate to pursue engagement opportunities with several stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

During Deployments

9.5. During deployments TVP must ensure that:

9.5.1. awareness raising measures are used in line with the TVP LFR SOP to ensure that the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed;

9.5.2. notices with a brief explanation and reference to the TVP website are available to hand out to the public on request; and

9.5.3. information is offered to persons engaged by officers in accordance with the policy referred to above.

After Deployments

9.6. After deployments ensure that:-

9.6.1. information about the deployment, including location, time, date, number of alerts, engagements, arrests, and any other information considered helpful and suitable for disclosure, is published on the TVP website. Care must be taken to ensure that no personal data is published; and

9.6.2. external engagement is considered in discussion with the TVP LFR team. Again, it may be appropriate to pursue engagement opportunities with several stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

10. WATCHLIST CONSIDERATIONS

Image Quality

10.1. The performance of the LFR system is heavily dependent on the quality of the images in the watchlist. Any images of insufficient quality will be technically prevented from extracting a biometric template and being uploaded into the LFR system. Whilst it will usually be the case that images populating the watchlist will have been previously collected in police custody, on a person's arrest, and are lawfully held by the police (and therefore likely to be relatively recent), it may be necessary to populate the watchlist with images that are not police held custody images, for example images of high risk missing persons provided by their families. In such cases, any anticipated use of non-police sourced images will be highlighted in the LFR Application. Code D of the Police & Criminal Evidence Act 1984 allows the images to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions. The best images are those that follow a custody or passport style image (e.g. full frontal face, neutral expression, uniform lighting and plain background).

Compiling the Watchlist

10.2. The TVP Legal Mandate provides commentary on the legal considerations relevant to compiling a watchlist in a lawful way, so as to ensure that TVP hold the watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes. The watchlist will be compiled, in its final form, no more than 24 hours before the first deployment.

10.3. Key points include ensuring the watchlist is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the watchlist.

10.4. The size of the watchlist is relevant to the level of resource that should be available to a deployment. There must be sufficient resource available to manage the alerts generated by the LFR application.

10.5. As explained in section 4 (LFR Overview), watchlist composition is normally restricted to individuals considered likely to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR deployment. An AO may deem it necessary and proportionate to authorise the inclusion of people to be included in a watchlist, even though there may not be specific intelligence to say where in TVP they might be found. The information or lack of information as to the likelihood of an individual being in proximity of an LFR deployment should be considered against a number of factors including: -

10.5.1. Severity of offence in question: this will often be relevant to the risk posed and / or the level of urgency associated with locating and arresting an individual as well as the anticipated impact on their conduct. Many individuals change their behaviour, including the places they reside and frequent when they know that they are wanted for a serious offence;

10.5.2. Risk: the level of risk associated with an individual or the offence type sought, whether that risk is to the public or themselves;

10.5.3. Deployment location: the specific characteristics of the deployment location, such as previous offending in the area (generally or specifically by the individual), local transport links and other amenities, may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the watchlist;

10.5.4. Offender: offenders suspected to reside in or frequent the relevant deployment location or whether no known residential address is available for the offender.

10.6. It is the responsibility of the LFR Silver Commander to ensure that reasonable steps are taken to ensure the quality of images included on the watchlist does not reduce the efficacy and accuracy of facial matching and, in this regard, ensure the following safeguards are implemented prior to deployment:

10.6.1. The most up to date custody images or non-police sourced images of a person who meets the criteria for inclusion on the watchlist will be extracted for LFR use.

10.6.2. By using image ‘ingestion settings’ (such as: distance between eyes, facial quality and facial reliability, face tilt) that have proven

to be reliable the LFR System has a technical safety net exist to prevent images of poor quality from being uploaded onto the LFR system.

10.6.3. Reviewing the proposed watchlist images prior to uploading, with particular attention paid to non-police sourced images (e.g.: for high risk missing persons), in combination with the briefing of LFR Operators and Engagement Officers enabling them to pay due regard to image quality and age when considering facial matching alerts.

Governing the Watchlist

10.7. The systems used to generate the watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

10.8. TVP LFR Documentation provides measures to ensure that the watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

10.9. 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.

Addressing disproportionality

10.10. TVP does not create or retain a breakdown of race, gender or any other protected characteristic[1] of persons on a watchlist. This mirrors the approach taken with most policing tools used by TVP. The exception here is for inclusion of under 18s and under 13s, where if their inclusion is anticipated, will be identified in the LFR Application. In order to ensure that appropriate consideration is given to the necessity and proportionality of their inclusion the watchlist will be reviewed, prior to deployment, to highlight persons under 18 for individual consideration. Only those persons deemed required strictly necessary and proportionate for inclusion for the purposes of the operation will be included.

10.11. The deployment of LFR is driven by a TVP identified policing objective that an intelligence-led evidence based assessment strongly suggests that it is necessary and proportionate to use LFR as a capability to locate specific individuals relevant to the objective. It is then the locality and policing objective that determines the composition of the watchlist. The individuals identified on a watchlist are there because there is a specific

[1] As defined in Section 4 of the Equality Act 2010.

policing need to locate them, there are realistic prospects of doing so, and that need fits with the policing objective driving the LFR deployment.

10.12. The routine retention of personal data relating to the protected characteristics of persons who are not matched by the LFR technology will not be retained. For the purposes of oversight and review of the use of LFR, TVP may utilise log data, which includes some personal data pertaining to matched facial images, together with other data held, including data relating to protected characteristics, where legally permitted to do so in order to provide assurance as to the ongoing efficacy and equitability of the LFR System. This will be retained for no longer than 31 days following the conclusion of the deployment. This log data may be de-personalised to remove any personal data, for longer term equitability analysis. This will then be retained in accordance with the LFR Retention Schedule.

10.13. TVP will continue to have regard to the published results of any academic equitability testing of the LFR system where necessary.

10.14. TVP has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. An example of such a bias is a system which is more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:

10.14.1. LFR is appropriately configured to minimise the risk of System Factors, having regard to the outcome of equitability testing detailed below;

10.14.2. those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and Environmental Factors throughout the Deployment. All persons involved should have received appropriate training and briefing. Should concerns arise that the LFR System is not performing correctly, the Silver Commander will halt the Deployment where necessary; and

10.14.3. for the purpose of facilitating post-Deployment reviews, Alerts are deleted as soon as practicable, but in any case within 31 days. This provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in place for the Deployment, including the reviews undertaken by Silver and Gold during the Deployment; and

10.14.4. in the event post-Deployment reviews identify an area of concern, TVP may undertake further equitability testing where this appears reasonably necessary.

11. DESIGN GUIDELINES FOR LFR

11.1. TVP LFR processes and associated guidance has been developed 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.

11.2. A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this guidance.

11.3. Directly relevant components include:-

11.3.1. the cameras, including cabling, and their placement;

11.3.2. the environment in which the cameras operate;

11.3.3. the database of reference images and associated meta data (the watchlist);

11.3.4. the facial recognition software that detects faces in the footage, converts the facial images into Biometric Templates, compares these against the watchlist and provides information to the Operator on the results of the comparison in the form of an audio and visual Alert, the two compared facial images side-by-side, and a numerical score;

11.3.5. the LFR Operator (who assesses Alerts) and the LFR Engagement Officer (who determines the appropriate course of action); and

11.3.6. having sufficient officer resource to support the deployment.

12. CAMERAS AND CAMERA PLACEMENT

12.1. Cameras must be selected so that the image resolution, frame-rate, field-of-view and low-level light performance can provide images of sufficient quality for use in the facial recognition application. Current FR systems typically require a facial image with between 20 and 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED).

12.2. Unless the environment is well controlled, cameras must be capable of operating at Wide Dynamic Range in order to generate high quality images under a variety of lighting conditions.

12.3. Cameras should ideally be positioned to capture faces as close as possible to the 'face-on' condition, similar to a passport image. This typically requires the cameras to be much lower than is normally the case for existing CCTV. Camera placement and angle should be further

considered where those sought may be more likely to be occluded in a busy crowd in order to maximise the prospects of location.

12.4. Ideally the environment should be managed such that every face is evenly illuminated. Highly directional lighting, for example strong sunlight, should be avoided, which may require consideration of how the lighting will change throughout the day.

12.5. In general, the Zone of Recognition will be smaller than the field of view of the camera; for example, not all faces in the field of view may be in focus and not every face in the field of view will be imaged with the minimum necessary Inter-Eye Distance (IED).

12.6. A typical 2MP camera will provide sufficient resolution for LFR to work on a maximum of 3 to 4 people side by side. Therefore, consideration needs to be given to camera location and the physical environment. For example, looking for opportunities to place the cameras to take advantages of physical features which funnel or restrict the movement of people within the Zone of Recognition. However, if the flow is reduced beyond a certain level, individuals may be grouped very close together, occluding or partly occluding the faces of people (people behind people).

12.7. The number of cameras used actively will be considered to ensure that the size and scale of the LFR deployment enables those on the watchlist to be effectively located without unduly processing biometric data.

12.8. Any deployment of LFR cameras will only take place where there is a reasonable likelihood (having regards to of identifying persons included in the watchlist. A range of factors will be relevant to this assessment and these include the nature of the site itself, available intelligence including previous criminality and the policing need to be at the site (including for the public's protection, supressing crime hotspots, and getting ahead of crime trends), watchlist composition and the perceived attractiveness of the location to persons of interest. Further considerations as to the appropriate location include the implications for human rights and the risks arising from collateral intrusion.

13. DEPLOYMENT LOCATION

13.1. The selection of a location for a deployment will be based on a number of countervailing factors including:

13.1.1. Intelligence regarding the previous criminality conducted in the relevant area, i.e. status as a crime 'hotspot' and/or by individuals on the watchlist;

13.1.2. Watchlist composition and nature of threat;

13.1.3. Nature of location, i.e. residential, commercial etc;

13.1.4. Local amenities, such as transport links, retail and leisure offering;

13.1.5. Local sensitivities, such as schools, medical facilities, religious or other cultural organisations;

13.1.6. Any anticipated demonstrations or other assemblies; and,/or

13.1.7. Availability of alternative routes.

13.2. The weight to be accorded to each of these factors will depend on and vary between each specific deployment.

14. KEY PERFORMANCE METRICS

14.1. This section covers some of the key performance metrics that should be gathered when deploying LFR. It outlines the minimum requirements and so additional metric or indicators may well be relevant and suitable for collation and analysis. There are two key metrics that determine the 'accuracy' of an LFR system. These are detailed in the below paragraphs.

True Recognition Rate (TRR)

14.2. The number of times when individuals on a watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times when these individuals passed through the zone of recognition (regardless of whether an alert is generated).

14.3. This metric can only be generated by 'seeding' known subjects (for example police officers or staff) into a Blue Watchlist and measuring the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated. Users of FR systems (and vendors) must not focus so closely on maximising this metric, that they increase the False Alert Rate to inappropriate levels.

False Alert Rate (FAR)

14.4. There are two types of False Alert Rate (FAR) measurements. The first is the System FAR, which is the number of False Alerts generated as a proportion of the total number of subjects processed by the LFR application. The second is the Operational FAR, which is calculated in the same way, but is measured after the LFR Operator has reviewed the output from the LFR application, and dismissed LFR application Alerts assessed by the LFR Operator as false.

14.5. All of the TRR and FAR metrics should be recorded and reported. Operational experience of other forces to date suggests that in most scenarios the FAR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the FAR is greatly affected by the number of subjects

processed by the LFR application, and to a lesser extent, the size of the watchlist. This is a key reason why the number of persons included on the watchlist needs to be kept as small as possible, whilst still meeting operational objectives.

14.6. It should be also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TRR and FAR. The Threshold needs to be set with care so as to maximise the probability of returning correct Possible Matches, whilst minimising the number of False Alerts. TVP will deploy LFR with a configured threshold of 0.64 demonstrating a low tolerance for false matches at a level which also minimises or extinguishes the risk of bias or discrimination. The accepted tolerance for false matches, is a False Alert Rate of 1:1000 which seeks to balance the countervailing interests in a proportionate way but in practice it is noted that at the configuration Threshold of 0.64, the FPIR/False Alert Rate performed significantly better both in scientific testing by the National Physical Laboratory and having regard to the operational experience of South Wales Police. In addition, the number of false alerts as a proportion of the total number of alerts is a potential measure of efficacy.

Recognition Time

14.7. A third important metric is the Recognition Time (RT). Note that the actual amount of time taken to act on an Alert will always be longer than the RT as additional time is needed for the LFR Operator to assess the Alert and to pass to an LFR Engagement Officer to then make a final decision on whether to Engage or not.

14.8. The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

15. LFR GUIDANCE SUMMARY

15.1. This guidance relates to the operational use of LFR, and the governance and oversight regimes necessary to support Deployment.

15.2. It is strongly advised that officers and staff adhere to the guidance as this will help ensure that TVP use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.

ACRONYMS USED IN LFR

AO	Authorising Officer
BSCC	Biometrics and Surveillance Camera Commissioner
CCTV	Closed Circuit Television
CIA	Community Impact Assessment
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EIA	Equality Impact Assessment
FAR	False Alert Rate
FR	Facial Recognition
FoIA	Freedom of Information Act
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LFR	Live Facial Recognition
MOPI	Management of Police Information
NPCC	National Police Chiefs' Council
NPL	National Physics Laboratory
RT	Recognition Time
SOP	Standard Operating Procedure
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition