Live Facial Recognition Standard Operating Procedure

Version History

No.	Date	Changes	By Whom
V0.1	10/12/2025	Initial Draft	Insp 957 Summers
V1.0	12/12/25	Review	Sharon Warwick Ben Gasson

Contents

1. Introduction

1.1. This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations. Compliance with the SOP will ensure a consistent response to the use of this policing tool.

2. Application

2.1. All Thames Valley Police (TVP), Joint Operations Unit (JOU) officers and police staff involved in the deployment of LFR will be made a aware of, and will comply with, all relevant TVP LFR policy and procedures. This will be completed through relevant training and briefing to those involved in the deployment of LFR. It will be emphasised to all officers and staff engaged in LFR Deployments that any perceived infringement of the rights of individuals, or failure to comply with the requirements of LFR documents, should be reported to the LFR Silver Commander.

2.2. The LFR Team within the Joint Operations Unit (JOU) are a collaborated unit made up of officers from both Thames Valley Police and Hampshire and Isle of Wight Constabulary with the relevant to authority to work across both forces. The TVP LFR deployments will be delivered using specialist equipment and officers within the 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 Legal Mandate, LFR Policy and LFR 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.

2.3. Commissioners should be aware of, and are required to comply with all relevant TVP policy and associated procedures.

2.4. This SOP applies in particular to officers and staff in the following roles: -

a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the planning and deployment of LFR technology; and

b) All police officers and police staff involved in any subsequent investigation resulting from the operational deployment of LFR technology; and

c) All Authorising Officers (AO); and

d) The operational command team for any LFR Deployment (Strategic, Tactical and Operational) and

e) LFR Operators, LFR Engagement Officer and LFR System Engineers.

Note: This list is not intended to be exhaustive.

3. Terminology

3.1. This SOP focuses exclusively on LFR.

Adjudication

A human assessment of an alert generated by the LFR 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 LFR application when a facial image from the video stream is being compared against the watchlist and returns a comparison (similarity) score above the threshold.

Application

Process that is used to request LFR Deployment in a certain area. This will present crime data, watchlist requests and rationale so the Authorising Officer can review.

Authorising Officer

An officer of the rank of Superintendent or above shall review the application and relevant documents to determine whether they can authorise the use of LFR. In an

urgent time sensitive matter, such as search of a murder suspect, the authorisation can be done an officer of the rank of Inspector or higher. This authorisation must be ratified by an officer of the rank of Superintendent or above.

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

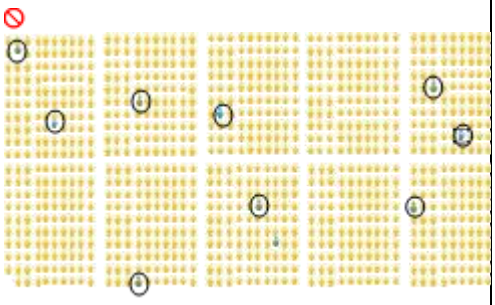
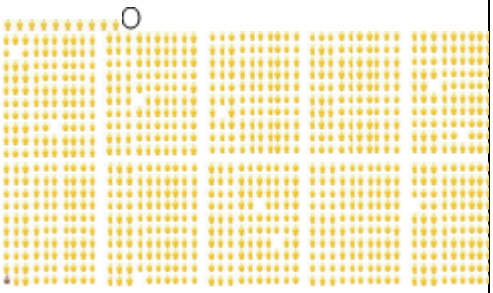
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

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, a single 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.

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 eg: 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 Documents

A suite of TVP strategic and deployment specific LFR governance documents which governs how TVP will use LFR as a policing tactic, many of which are published to enable the public to foresee how LFR will be used by TVP. They include: LFR Legal Mandate, LFR Policy, LFR Standard Operating Procedure, Equality Impact Assessment, Human Rights Impact Assessment, Surveillance Camera Code of Practice Self-Assessment, Data Protection Impact Assessment, LFR specific Privacy Notice, LFR specific Appropriate Policy Document, LFR deployment specific Application and Authorisation and LFR deployment specific record keeping logs.

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.

Operational Plan.

Completed by the LFR Team to ensure that appropriate risk are identified and officers are briefed on the Operation.

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. Authority to Deploy LFR

4.1. In normal circumstances, the authority given by an AO to deploy LFR in support of a Policing Operation should be made by an officer not below the rank of Superintendent. Their authorisation should be recorded in writing.

4.2. The TVP LFR Application / Written Authority Document recognises that the intelligence case for the use of LFR may give rise to a single deployment, or a need for a series of deployments within a time-limited period. Where the TVP LFR Application / Written Authority Document is to be used to authorise a series of deployments, the dates will be detailed as part of the application and will not be for more than a single 7 day period. A further Authorisation will be needed for a deployment longer than 7 days or a further deployment period.

4.3. 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.

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

4.5. TVP will have independent oversight as an individual force for applications and Authorities. The operational deployment will be managed by the Joint Operations Unit (JOU) LFR Team. Relevant records of process and deployments will be held within the JOU.

4.6. Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable.

4.7. Currently, the only circumstances in which AO will authorise deployment of LFR to locate persons of interest are set out below. This may change as TVP's approach to LFR evolves, in which case the LFR Legal Mandate, LFR Policy and this LFR SOP and other related LFR documentation would be reviewed and updated accordingly.

4.7.1. 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.

4.7.2. 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.

4.7.3. 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.

4.7.4. 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.

4.8. The authority of the AO: -

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; 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 a proportionate means of achieving the legitimate aim of the deployment;

d) must, from a Data Protection Act 2018 perspective, articulate why it is strictly necessary for TVP 's law enforcement purposes; meaning there is a `pressing social need' and it is not reasonably viable to address this through less

intrusive means, either because less intrusive tactics have been tried, or it is reasonably believed that those tactics are unlikely to be effective). Details of the applicable requirements are set out in both the LFR Data Protection Impact Assessment and the LFR Legal Mandate for reasons of substantial public interest; and

e) must articulate that the AO has given regard to the safeguards proposed for the Deployment and the safeguards contained within the TVP LFR Documents, and considers based on the information therein that the deployment in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the Data Protection Act 2018 and UK GDPR; and

f) means that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the watchlist complies with TVP LFR documents, including the legality, necessity and proportionality criteria; and

g) means that the AO considers that the Deployment is proportionate, with the benefits anticipated from the use of LFR outweighing the concerns and impacts there may be in relation to people's data protection rights, human rights and rights relating to equalities; and

h) means that the AO is satisfied that the control measures in the Data Protection Impact Assessment, Community Impact Assessment, and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the Deployment

i) means the AO has determined the minimum Threshold setting to be utilised during the Deployment. This setting will be where no facial recognition system bias is detected (currently 0.64 with the TVP LFR algorithm used).

4.9. In cases of urgency an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency. All authorisations must comply with the requirements set out in above paragraph

4.10. Situations where the need for an authorisation to be granted urgently would include for example: an imminent threat to life or serious harm to people or property.

4.11. If an authorisation is given under the urgency criteria above, it shall be the duty of the AO who gives it, to inform an officer of the rank of Superintendent or above as soon as practicable, that LFR has been deployed and the reasons

why. It is for the Superintendent to then authorise the deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

4.12. Should a further law enforcement purpose that necessitates a change to the authorised watch list be identified after the AO has issued their authority for an LFR deployment, changes to the watch list are not permissible unless an AO grants a further authority for it.

5. Where – Date, Time, Duration and Location of Deployment

5.1. The AO should define the date, time, location and duration the Deployment is authorised for based on the principle of necessity and proportionality in pursing a legitimate policing aim, informed by the intelligence case behind the deployment.

Considerations relevant to an LFR Deployment Location

5.2. The chosen location for the LFR deployment will be determined by: the intelligence case objectives of the deployment and the Community Impact Assessment.

5.3. The deployment location will be determined by there being reasonable grounds to suspect that the proposed deployment location is one at which one or more persons on the watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any deployment locations should be recorded and be capable of being considered and evaluated by an objective third person.

5.4. The selection of a deployment location may be further supported by:

a) Policing information or intelligence about a proposed deployment location including if there is an increased public safety risk at a location, *and*

b) The ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so.

5.5. When reviewing a deployment location, AO's must also consider which persons and categories of person are likely to pass the LFR system and:

a) The reasonable expectations of privacy the public may have at that location. Some places by their nature attract greater privacy expectations than others, for example, the expectations at a busy public transport hub being different to that of a quiet suburban park of backstreet. The number of cameras used by the LFR system should also be considered in this context to ensure the size

and scale of the deployment enables those on a watchlist to be effectively located without processing excessive biometric data.

b) Whether a proposed deployment location is likely to have an impact on a specific community or group of people because of its proximity to a particular location or facility. Examples of such locations[1] could be:

    i. Hospital, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), medical treatment settings, care homes and persons who may be attending a nearby assembly or demonstration are examples where those that attend them may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area.

c) Consideration should be given to the alternative routes and their accessibility for persons who do want to walk through the Zone of Recognition.

5.6. Where it is practicable to identify a person of being responsible for a proposed deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where an LFR deployment and / or location may engage wider human rights issues and as appropriate.

5.7. Where privacy or other human rights considerations are identified in relation to a particular deployment, the AO needs to consider the necessity to deploy LFR to that location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is necessary, AO's need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR system against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.

Measures during an LFR Deployment

5.8. During any policing operation where LFR is deployed in line with TVP LFR SOP, signs publicising the use of technology should be prominently placed in advance of the Zone of Recognition. These measures are to alert members of the public to the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition.

[1] Should a deployment be necessary at a site that is focused on children (for example outside a school), signage and information about the LFR deployment should typically be reasonably accessible to children who may pass through the zone of recognition. Consideration is needed as to the nature of the deployment and data processing that is proposed and the effectiveness of mitigations when assessing if the deployment is proportionate.

5.9. TVP will notify the public in advance of LFR deployments using force websites and other appropriate communication channels (including social media). In exceptional circumstance the advance notice given may be reduced due to operational imperative of the Deployment (for example, in cases of urgency or where it would compromise other policing tactics). An example of when providing shorter notice publication to the public, would be a known person wanted for murder, or other similar very serious offences, with intelligence that they will be in a particular area.

5.10. If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of a policing power. TVP staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics. This could include powers available to police in normal circumstances, such as:

5.10.1. Section 1 PACE 1984 power to search, with suitable grounds. An example would be, an officer has reasonable grounds to suspect someone is on possession of stolen items.

5.10.2. Section 60 and 60AA of Criminal Justice and Public Order Act 1994, authority to search and remove face coverings, authorised by an Inspector or above with specific criteria. An example of Sec 60 and 60AA – Intelligence of serious disorder in a location, a Police Inspector or above ranks can authorise, if they reasonably believe, officers to conduct stop and search for weapons to prevent the disorder, for no more than 24 hours. The officers searching do not need to have their own grounds for this search. Whilst the Section 60 above is in place a Police Inspector or above can authorise Section 60AA for the removal of any item that the searching officer reasonably believes that person is wearing for the purpose of concealing their identity.

5.11. Any member of the public who is engaged as part of an LFR deployment will be offered an information leaflet about the technology.

6. 'Who' – Watchlist generation and criteria for an image's inclusion on a Watchlist

6.1. This section covers the composition, generation and management of Watchlists to be used in LFR deployments and is structured to address:

a) Safeguards relevant to all Watchlists – including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics;

b) Who may be added to a Watchlist – including in relation to police-originated, and non-police originated imagery;
c) The approach to be taken to additional Watchlist categories – this being relevant where the need to undertake a deployment is already made out by reference to the primary Watchlist and the intelligence case supports the use that the deployment to locate further persons, for example those wanted by the courts – such additional purpose must also be necessary and proportionate.

Safeguards relevant to all Watchlists

6.2. The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria provided by the TVP LFR: Legal Mandate, Policy and this SOP; and be specific to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:

Requirement	Rationale for the requirement
Intelligence: Watchlists must be driven by a policing objective and based on the intelligence case. The intelligence case must be current and reviewed before each deployment	This intelligence driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR deployment
Images Sources: Watchlists must only contain images lawfully held by police with consideration also being given as to: • The legal basis under which the image has been acquired; *and* • The source of the image, particularly where the image is derived from a sensitive or third party source and may risk compromising that source of exposing that source to risk.	This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases the lawfulness and privacy intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance.

	Additionally policing has a responsibility to avoid compromising policing tactics or exposing sources to risk – this requirement covers this point
Image Selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: • is of a person intended for inclusion on a given Watchlist; and; • is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator).	This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The TVP Senior Responsible Officer for LFR has determined the 1:1000 false alert rate represents an approach which balances these factors in a proportionate way.
Watchlist currency: Watchlists must not be imported into the LFR system more than 24 hours prior to the start of the deployment.	This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours
Watchlist Design: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate

	action is taken should an Alert be generated.

Additional safeguards relating to protected characteristics

6.3. Following on from the Bridges – V – Chief Constable of South Wales Police case, in December 2020 the then Surveillance Camera Commissioner (SCC) published his best practice guidance document 'Facing the Camera'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist. Any controls, mitigations and processes identified in this document reflect TVP's LFR System performance and particular use cases for LFR.

6.4. TVP has confidence in the LFR system's performance, particularly in relation gender, age and race.

6.5. TVP provides that in the creation of the watchlist for each Deployment, where source data allows, TVP must specifically identify and make the LFR Team specifically aware that the Watchlist contains persons who are believed or suspected to be:

a) Aged under 18 years old;
b) Aged under 13 years old;
c) A person with a relevant disability[2];
d) A person who has undertaken a gender reassignment and it is believed or suspected to be, that the Watchlist would be using an image of that person prior to their reassignment.

6.6. Safeguards regarding composition: The following outlines further, specific safeguards that apply to the composition of the Watchlist:

	Age (U.18)	Age (U.13)	Disability	Gender Reassignment
Circumstances				
	LFR is used to locate a person under 18 and that	LFR is used to locate a person	LFR is to be used to locate a person and that person's	LFR is to be used to locate a person and that person's records state that person has

[2] A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) and that such a disability may impact on the performance of the police force's LFR system. Examples which may have an impact (depending on the performance characteristics of the specific LFR system) include if the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised.

	person's records state that person is aged (or suspected to be aged) under 18-years-old	under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old	records state that person has (or is suspected to have) a relevant disability	(or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the watchlist would be using an image of that person taken prior to their reassignment
Safeguards				
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with TVP LFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images	There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the watchlist			
Technical Advice	Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist and make the LFR Operator aware of any such limitations. Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be blocked from the camera's line of sight. Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.			

Police-originated images that may be included on a Watchlist

6.7. Images that may be deemed appropriate for inclusion within an LFR Watchlist include custody images of individuals and/or police originated images other than custody images of people who are:

(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.

6.8. Where police originated images other than custody images considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a policing objective and the proportionality of using such images on an LFR system

Non-police originated sources of Watchlist imagery

6.9. Where it is viable to do so without unduly impacting on the performance of the LFR system, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by TVP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of non-police originated image.

6.10. There may be occasions, where no image is held by TVP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of non-police originated image. For the avoidance of doubt, this policy does not provide a basis to proactively acquire images solely for use on an LFR Watchlist.

Assessing Non-police originated sources of Watchlist imagery

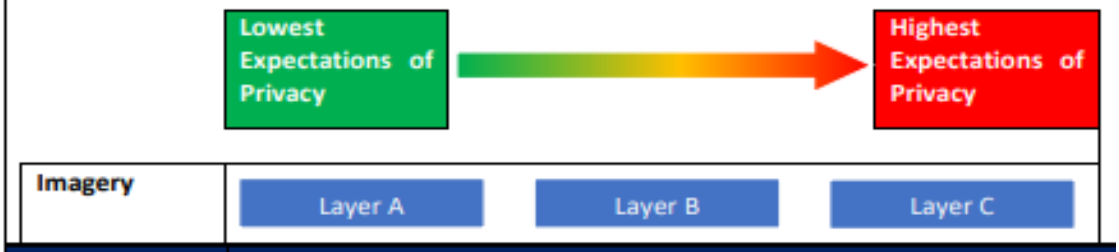


Image Layer	Outline
Non-police originated image – **Layer A**	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage; • circumstances where the police have obtained the image as a result of a lawful power of search or seizure; • data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.
Non-police originated image – **Layer B**	Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject, including any imagery obtained pursuant to: • the Regulation of Investigatory Powers Act 2000; and • the Investigatory Powers Act 2016, where the ability of relevant bodies to obtain such images is further supported and can be anticipated by reference to published Codes of Practice.
Non-police originated image – **Layer C**	Non-police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received. To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.

6.11. Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular which layer of intrusiveness the image is attributable to and the factors at paragraph 6.10 above.

6.12. The types of non-police originated images that may be deemed appropriate for inclusion within an LFR Watchlist are of people:

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.

6.13. '**Missing persons deemed high risk'** – This term will be subject to the College of Policing definition of that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed highly likely and serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.

6.14. The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
b) the importance of locating the person or people sought with references to the threat, harm, opportunity and risk[3] (THOR) which the addition to the Watchlist addresses;

[3] Including for the purposes of taking preventative measures against the occurrence (or future occurrence) of the relevant threat, harm, opportunity and risk

c) whether the significance of the THOR identified, which inclusion on the Watchlist would address outweighs any expectations of privacy.

7. TVP LFR Documents

7.1. **Assessments;** For each authorised LFR operation, the following assessments need to be created, and amended where necessary;

- **(i)** Data Protection Impact Assessment* (Review/Amend/Adopt); and
- **(ii)** Equality Impact Assessment* (Review/Amend/Adopt); and
- **(iii)** Community Impact Assessment* (carry out); and
- **(iv)** The Surveillance Camera Commissioners Self-Assessment* (Review/Amend/Adopt); and
- **(v)** LFR Operational Risk Assessment (carry out)

**Note: ***Any assessment listed above showing 'Review/Amend/Adopt' has already been created by the TVP LFR team. Each will require case by case consideration to ensure the document remains appropriate and sufficient for each LFR operation. Assessments should remain under continual review to ensure the Deployment falls within them and they remain sufficient for the circumstances as they evolve.

8. Risk Assessment & Resource Levels

8.1. Each Deployment should be risk assessed and the appropriate risk assessment documents completed. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.

8.2. The level of resources, including back-up contingencies, required to support each deployment is a matter to be determined by the operations command team.

8.3. Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.

8.4. LFR system engineers will be deployed to support LFR deployments and will come with suitable vehicles where required.

8.5. All TVP officers and staff deployed on LFR Deployments must be compliant and in date with their force's First Aid and were applicable Officer Safety (PPST) training requirements.

9. Planning & Booking

9.1. As part of the LFR planning process and before the AO authorises a Deployment, the TVP LFR team should be consulted on the appropriateness and viability of a deployment.

10. LFR Operational Roles

LFR Command Team

10.1. LFR Deployments must be supported with a clear command structure. The following roles are defined for the purpose of creating an appropriate hierarchical command structure:

~~a.~~ Gold Commander (Superintendent or above); There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their `strategic intention' aligns with the Written Authority Document. Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold will also liaise as necessary with NPCC ranked officers.

b. Silver Commander (Inspector or above); There is only one Silver Commander for any LFR Deployment. Silver reports to Gold. Silver has tactical command of the Deployment and is responsible for tactical implementation. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having regard to the effectiveness of the safeguards in place whilst LFR is being used.

c. Bronze Commander, Officers from the LFR Team or Sgts and above with suitable knowledge of LFR; Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with

sufficient clarity, and ensure that they are fully understood by all officers and staff involved in the Deployment.

10.2. Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative command team terminology, or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

LFR Operator

10.3. LFR Operators receive detailed training prior to being deployed operationally. Their role is to monitor and assess system Alerts, before working with LFR Engagement Officers (as necessary) to decide whether an Engagement is required.

10.4. The LFR Operator should log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR system performance (be it generally or in relation to specific Watchlist images) to the Silver Commander.

10.5. The LFR Operator's Deployment Record should include:

a) The LFR operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; *and*
b) what decision was taken regarding whether to Engage a member of the public or not; *and*
c) whether an Engagement was successfully undertaken, and the outcome of the Engagement

LFR Engagement Officer

10.6. LFR Engagement Officers must have an understanding of the LFR system, how it performs, and what effect Subject, System, and Environmental Factors might have. These officers must receive a full operational briefing prior to deployment. These officers will be deployed in uniform.

10.7. When conducting an Engagement, LFR Engagement Officers must ensure that they do so lawfully, and in an appropriate and proportionate manner. Officers must comply with the Code of Ethics at all times. Members of the public who have been subject of an Engagement, will be supplied with an LFR information leaflet.

10.8. The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place. It must not be an automatic consequence that an Alert results in an Engagement.

10.9. When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal.

10.10. Whilst officers must exercise their own discretion when using their powers of arrest and detention, TVP's policy is that an LFR system-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

10.11. If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

10.12. After any Engagement (that follows an Alert), the LFR Engagement Officer must update the LFR Operator with the outcome of that Engagement.

10.13. Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, cannot or should not engage with a member of the public as they would do in any other set of circumstances if someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so. Simply turning away from Zone of Recognition is not suspicion to stop and engage with a member of the public.

11. In advance of an LFR Deployment:

11.1. Deployments will only use suitably trained, qualified and briefed officers and staff, as described in Section 10.

11.2. LFR Deployments are notified to the public using TVP Website and other suitable communications, such as social media.

11.3. LFR Awareness raising measures are ready for deployment. Signs are place outside the Zone of Recognition.

11.4. Suitable LFR information leaflets are available, to be given to public that police engage with following an alert.

11.5. 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;

11.6. External Engagement is considered in discussion with 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.

12. During Deployment

12.1. A site assessment will be completed by an LFR Operator on the day of deployment. The site assessment will ensure no change to the layout of the area or a new property or premise that would require another review by the AO or Termination of deployment. This would include for example a building being used as a School, Place or Worship, Hospital, Polling Station or a Demonstration or Assembly.

12.2. Operators will record relevant details, such as weather, suitable light levels and location of signage.

12.3. Operators will complete confidence checks of the system, as per their training. This will be done by walking through the Zone of Recognition waiting for a match from an image of the team member walking through.

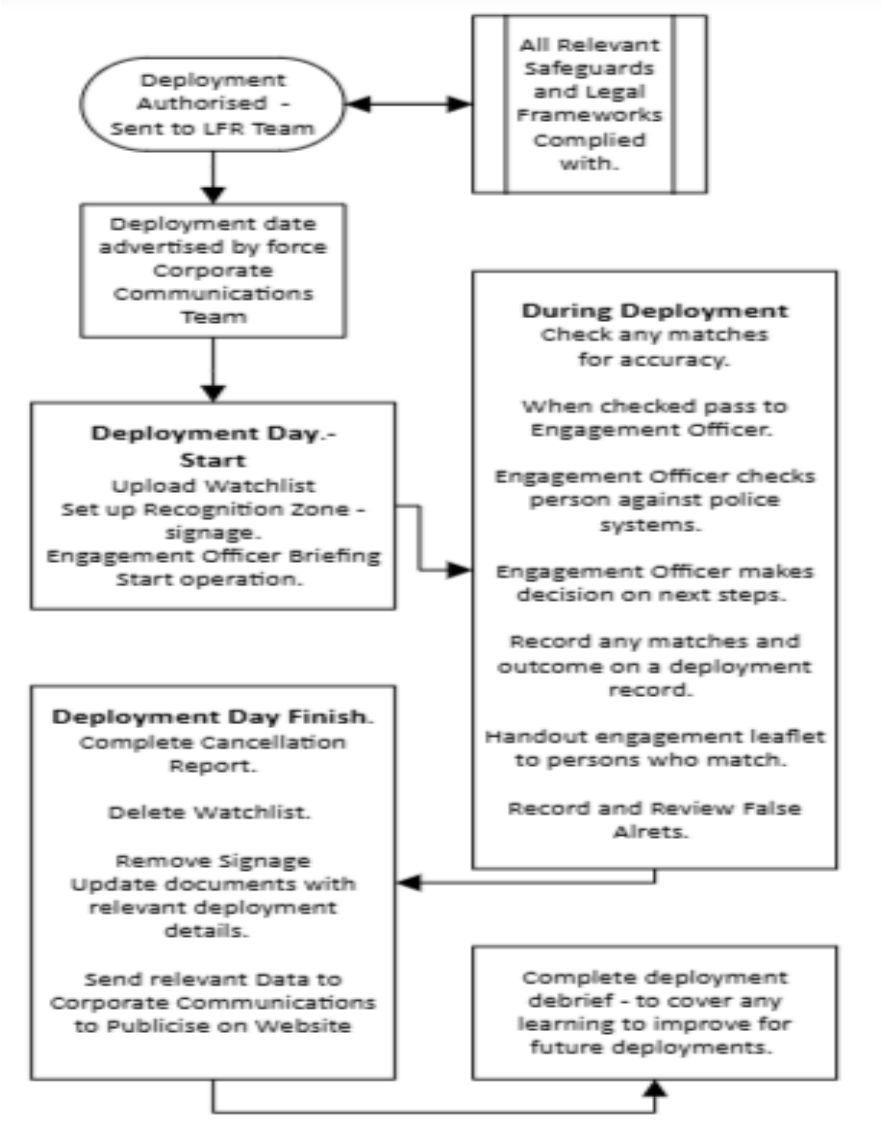
12.4. If there is an issue with the LFR equipment that is directly involved in the capture of biometric data the LFR Operator will halt the operation to determine the issue. If it is not possible to rectify the issue the operation will end and advice from National Police Chiefs Council and LFR system provider will be sought before a further deployment. This will be recorded and shared with LFR Silver Commander to escalate if required.

12.5. All officers and staff involved will deploy for the time period allowed under the authorisation.

12.6. It will be emphasised to all officers and staff engaged in LFR Deployments that any perceived failure to comply with the requirements of LFR documents or infringement of the rights of individuals, must be reported to the Silver Commander.

12.7. Details of engagements and outcomes will be passed to the LFR Operator to be recorded.

13. Flow Chart of Deployment process:



14. Post Deployment

14.1. In furtherance of TVP paying due regard to its ongoing Public Sector Equality Duty, following each LFR Deployment, the Silver Commander must ensure that a post Deployment evaluation is completed which is updated in the Deployment Record. The evaluation process must capture an assessment of the operational effectiveness and equitability of the LFR Deployment. This evaluation should be both qualitative and quantitative in nature.

14.2. The evaluation should clearly articulate what measures are used to assess the operational effectiveness and equitability and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the Deployment and what opportunities exist to improve them for future use, and how learning will be shared.

14.3. 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.

15. Data Retention & Data Management

15.1. TVP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the TVP LFR Documents. This means that:

a) where the LFR system does not generate an Alert, that a person's biometric data is immediately automatically deleted; and
b) the data held on the encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable and in any case within 24 hours after the end of the deployment.

15.2. Where the LFR system generates an Alert, all biometric data is deleted as soon as practicable and in any case within 24 hours after the end of the deployment.

15.3. Any CCTV footage generated from LFR Deployments is deleted after 31 days, except where retained:

a) Due to its relevance in a criminal investigation and is held in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
b) in accordance with TVP's complaints / conduct investigation policies.

15.4. To support compliance the LFR system has an audit capability, and the deployment logs are retained in accordance with TVP LFR Document Retention Schedule which is referenced in the TVP LFR specific Appropriate Policy Document. The LFR Team are responsible for the retention and deletion of LFR data used and collected in LFR deployments, in accordance with the LFR Retention Schedule.

Register of Deployments

15.5. Any deployment of LFR must be recorded on a centrally held register. This register will record a number of things including:

a) Name and rank of the AO and command team; and
b) Date, time, duration, and locality of deployment; and
c) Watchlist composition statistics (not including any personal data); and
d) The number of match alerts and demographic breakdown relating to these (not including any personal data);
e) Number of engagements and their results.

15.6. TVP will make non-personal information relating to LFR Deployments available to the public in accordance with the TVP LFR Documents.

16. Further Documentation

16.1. Further documentation is available providing useful information relevant to LFR. This is detailed below.

a) Information Management APP; https://www.college.police.uk/app/information-management
b) National Decision Model; https://www.college.police.uk/app/national-decision-model

c) National Intelligence Management; Intelligence management | College of Policing
d) College of Policing Code of Ethics; https://www.college.police.uk/app/national-decision-model/national-decision-model
e) Home Office Biometric Strategy – Published June 2018; https://www.gov.uk/government/publications/home-office-biometrics-strategy
f) High Court Ruling – R (on the application of Edward Bridges) v The Chief Constable of South Wales (2019) EWHC 2341 (Admin); High Court Ruling