METROPOLITAN POLICE

More Trust | Less Crime | High Standards

MPS LFR POLICY DOCUMENT

Direction for the MPS Deployment of overt Live Facial Recognition Technology to locate person(s) on a Watchlist

Table of Contents

Terms & Definitions: Capitalised terms used within this LFR Policy Document shall have the meaning given to them in section 3 of this document unless otherwise defined.

1 Introduction, Aim and Scope

Introduction

1.1 Live Facial Recognition (LFR) is used by the Metropolitan Police Service (MPS) as a precision crime-fighting tactic to locate people who are wanted by the MPS and/or the Courts. It helps us keep Londoners safe. More detail about how LFR works and how the MPS uses it can be found in section 4 (LFR Overview).

1.2 This MPS LFR Policy Document provides MPS personnel with direction on the overt use of LFR to locate those on a Watchlist in a legally compliant and ethical manner to enable the MPS to achieve legitimate policing aims.

1.3 This document specifically addresses a number of recommendations made by the London Policing Ethics Panel (LPEP) in their May 2019 report on the use of LFR. The MPS is also cognisant of the views and ongoing considerations of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner.

Aim & Scope

1.4 This document aims to:-

a) provide MPS personnel and members of the public with information about the MPS's present strategic, operational and technology objectives for the overt use of LFR to locate those on a Watchlist, such that its enables the MPS to achieve its law enforcement purposes and is compliant with key LPEP recommendations (the Objectives); *and*

b) provide MPS personnel with direction on the construction of Watchlists and the Deployment of overt LFR technology by the MPS in spaces accessible to the public in order to meet the MPS's Objectives for LFR; *and*

c) establish the governance structure for the Deployment of LFR, ensuring that MPS use of LFR is appropriately governed and legally compliant; *and*

d) provide an overview of LFR technology and advise on practical issues such as camera selection and placement in order to obtain the best performance from the LFR system; *and*

e) as part of a published suite of documents, assist the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the MPS, as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

1.5 This document relates only to the MPS's use of overt facial recognition (FR) technology to locate person(s) on a Watchlist. Facial recognition technologies have a number of potential applications within a law enforcement context. These deployment methodologies and the names adopted for each by the MPS are summarised in the table below in order to provide MPS personnel and the public with an overview of terminology, as well as to ensure precision and consistency when referring to various facial recognition technologies.

FACIAL RECOGNITION OVERVIEW				
Facial Recognition – Method of use:		The use of facial recognition where all people passing the system's camera(s) are analysed by the system with results being generated at the same time as events.	The use of facial recognition where: (i) media is directly captured of a subject present; or (ii) media is otherwise acquired in lieu of capturing it, with the intent of subjecting it to analysis by the facial recognition system. The results of such analysis could shape events to which the footage relates in real time.	The use of facial recognition where media is analysed after the event. The result of such analysis would come sufficiently after the event such that they could not shape events to which the media related in real time.
Overt	**Name**	Live Facial Recognition (**LFR**)	Operator Initiated Facial Recognition (**OIFR**)	Retrospective Facial Recognition (**RFR**)
	How it may be referred to:	*"... the use of overt live facial recognition to locate people on a watch list who are sought by the police …"*	*"... the use of operator initiated facial recognition which takes an image of a particular person and uses it to either (i) help policing establish who a person in the image is or (ii) establish where a person has previously appeared in other media held by the police ..."*	*"… retrospective facial recognition may be used after an event to help officers establish who a person is or whether their image matches against other media held on databases ... "*
Covert	**Name**	Covert Real-Time Facial Recognition Surveillance (**CRFRS**)	Covert Operator Initiated Facial Recognition Surveillance (**COIFRS**)	RFR is not a covert capability in itself. It may however use media obtained via covert means.
	How it may be referred to:	*… "whilst the then Surveillance Camera Commissioner has recognised a possible application for facial recognition in a covert way, subject to the Regulation of Investigatory Powers Act 2000, policing does not comment on any potential use of covert policing tactics …"*		

1.6 The potential need for FR to be used covertly has been acknowledged by the then Surveillance Camera Commissioner in his December 2020 guidance, 'Facing the Camera'. The MPS is cognisant of its responsibilities under the Regulation of Investigatory Power Act 2000 (RIPA) and the training for the overt use of FR deployments includes providing the AO with assistance on

recognising where RIPA may apply when using FR. Further guidance on RIPA can also be obtained from the MPS MO5 - Covert Governance. Whilst the MPS does not confirm nor deny any covert use of FR, and the possibility is included in the summary table to help distinguish it from overt deployment methodologies, any potential covert use of FR would be beyond the scope of this document.

Not in Scope

1.7 This document does **not** extend to:-

a) manually instigated facial recognition for retrospective searching of video / still images - RFR; *or*

b) operator initiated facial search submitted from a mobile device (or similar) in near real-time - OIFR; *or*

c) tracking a person's movements around the country across a number of camera systems; *or*

d) any covert use of FR systems including CRFRS and COIFRS; *or*

e) any MPS use of third-party owned or operated FR systems, 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 document*; or*

f) the legal framework that is applicable to the MPS's use of LFR – this is separately detailed within the MPS's Legal Mandate document.

Additional Documents

1.8 A number of documents are available to supplement this document and these include the:-

a) LFR Authorisation Process Guidance Flowchart (produced by DLS to provide legal advice for applicants and AOs);

b) LFR Human Rights Consolidated Guidance (produced by DLS to provide legal advice for applicants and AOs);

c) MPS LFR Standard Operating Procedure (SOP);

d) MPS LFR Data Protection Impact Assessment (DPIA);

e) MPS Facial Recognition Technology: Understanding accuracy and demographic differences;

f) MPS LFR Training Document (PowerPoint).

2 Document Edit History

2.1 As a living document, this MPS LFR Policy Document will be subject to periodic review, on at least an annual basis. It is likely to be amended as the technology develops further and as the circumstances relating to LFR Deployment evolve.

Version	Date	Additions/Modifications
Version 1.0	24/01/2020	Original document.
Version 2.0	29/11/2021	Updates as a part of a periodic review, incorporating points of clarification, facial recognition terminology/overview and consolidating points made elsewhere by the MPS.
Version 3.0	20/03/2023	Updates as a part of a periodic review.

3 Terminology

3.1 Within the MPS and throughout the MPS LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition:

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
Administrator	means a specially trained person who has access rights to the LFR application in order to optimise and maintain its operational capability. The Administrator may also be referred to as the LFR System Engineer.
Alert	means the Alert generated by the LFR system when a facial image from the video stream, which is being compared against the Watchlist, returns a comparison (similarity) score above the set Threshold.
Application	sets out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.
Authorising Officer (AO)	is the officer who provides the authorisation for LFR to be Deployed. LFR may not be used without this authorisation.
Biometric Template or Template	is 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. Note that Templates are proprietary to each facial recognition algorithm and new Templates will need to be generated from the original images if the algorithm is changed.
Blue Watchlist	is a Watchlist comprising of 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 at the start of a Deployment to measure the True Recognition Rate.
Bronze Community	is appointed by Silver specifically to oversee and manage community engagement and issues relevant to an LFR Deployment or a series of LFR Deployments in a defined area.

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
Cancellation Report	records details of where and when a Deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.
Candidate Image	means the image of a person from the Watchlist return as a result of an Alert.
Confirmed False Alert	means, following an Engagement, it has been determined that the Engaged individual is not the same as the person in the Candidate Image in the Watchlist.
Confirmed True Alert	means, following an Engagement, it has been determined that the Engaged individual is the same as the person in the Candidate Image in the Watchlist.
Deployment	means use of an LFR system as authorised by an AO to locate those on an LFR Watchlist.
Deployment Record	means collectively; • the Application (seeking approval for the LFR Deployment); • the Written Authority Document (provides a record of the decision making by the AO to give authorisation to deploy LFR); and • the Cancellation Report (recording details and results from an LFR Deployment).
Engagement	occurs when an officer communicates with a member of the public as a result of an LFR Alert. The term 'Engagement Officer' shall be construed accordingly.
Environmental Factor	is an external element that affects LFR system performance such as dim lighting, glare, rain, mist etc.
False Alert	means that it is determined that the Probe Image is not the same as the Candidate Image in the Watchlist, based on Adjudication without any Engagement.
Faces per frame	means a configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
Facial Recognition (FR)	Is a technology which works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database generating possible matches. This is based on digital images (still or from live camera feeds).
False Alert Rate This is also known as the False Positive Identification Rate.	describes 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.
False Negative	Is where a person on the Watchlist passes through the Zone of Recognition but no Alert is generated. There are a number of reasons False Negatives occur, and these include System, Subject and Environmental Factors, as well as how high the Threshold is set.
Gold Commander	is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment.
Live Facial Recognition (LFR)	is an overt real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined Watchlist in order to locate Persons of Interest by generating an Alert when a possible match is found.
LFR Engagement Officer	means an officer whose primary 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 help understanding of the purpose and nature of the LFR Deployment.
LFR Operator	is the officer / member of staff operating the LFR application. They will consider Alerts, and via the Adjudication process, assist LFR Engagement Officers in deciding whether an Alert should result in further action or not.
LFR System Accuracy	is not defined by a single figure to measure the accuracy of an LFR System – accuracy is determined by an overall assessment

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
	of two metrics, the True Recognition Rate and the False Alert Rate.
MPS LFR Documents	means the `Level Three' MPS LFR Documents that regulate the MPS use of LFR, as more particularly identified within the MPS LFR Legal Mandate.
Primary Watchlist Category (PWC)	is the category of images on the Watchlist that directly support the primary purpose of the Deployment.
Probe Image	means the facial image submitted for a facial search against the Watchlist.
Recognition Opportunity	means the period when a person's face is visible to a LFR camera(s) as they move through the Zone of Recognition.
Recognition Time	means the average time from when a face appears in the Zone of Recognition of the camera to when the LFR system generates an Alert.
Silver Commander	is the officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander.
Subject Factor	means a factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.
System Factor	means a factor relating to the LFR system such as the algorithm.
Threshold	means 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 correct suggested matches whilst keeping the number of False Alerts to an acceptable level. (NB. It should be noted that any FR algorithm is only returning 'suggested' matches, based on the chosen Threshold, and that it is for a human to assess the true likelihood that the images relate to the same person.)
True Alert	is when it is determined that the Probe Image is the same as the Candidate Image in the Watchlist.

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
True Recognition Rate This is also known as the True Positive Identification Rate	describes the total number of times an individual(s) known to have passed through the Zone of Recognition and correctly generated an Alert, *as a proportion of* the total number of times the same individuals pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR system or not. By way of an example, the 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. The same would be true if 5 people each pass the LFR system twice, and 2 Alerts were correctly generated for 4 of the people and only 1 correct Alert for the 5th person.
Urgency	means, 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 opportunities with limited time to act, where the seriousness and potential benefits support the urgency of action.
Watchlist	means the 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 (for example a police force's custody image dataset) and will have been created specifically for the LFR Deployment. The criteria for inclusion of images in a Watchlist will be determined by the intelligence, data and analysis available, as well as the policies outlined in this document.
Written Authority Document (WAD)	provides the decision making audit trail demonstrating how the MPS LFR AO has considered the legality, necessity and proportionality of the Deployment, the safeguards that apply to the Deployment, and the alternatives that were considered but deemed to be less viable in realising the policing purpose. It also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the Deployment.
Zone of Recognition (ZoR)	means 3-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

Adjudication	means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).
	smaller than the field of view of the camera, e.g. 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 the Metropolitan Police Service (MPS) as a precision crime-fighting tactic to locate people who are wanted by the MPS and/or the Courts. It helps us keep Londoners safe.

4.2 LFR helps us 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 images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. Watchlist composition is normally restricted to individuals suspected 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.

4.3 LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify possible matches against persons of interest to LEAs.

4.4 Where the LFR system identifies a potential image match, the LFR system flags an Alert to a trained member of MPS personnel who then makes a decision as to whether any further action is required. In this way, the LFR system works to assist MPS personnel to make identifications rather than acting as an autonomous machine based process devoid of user input.

LFR and the MPS

4.5 The MPS believes that LFR is a valuable precision policing tool that helps the MPS 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.

4.6 The following are illustrative examples where LFR may assist the MPS with its policing purposes:-

a) Supporting the location and arrest of people wanted for criminal offences;

b) Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders);

c) Supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons deemed at risk etc.);

d) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.

4.7 Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. The MPS is conscious that the use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, 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 the MPS to ensure that LFR is used lawfully 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, the MPS has facilitated academic research led by the University of Essex, and has proactively engaged with civil liberty interest groups, the London Policing Ethics Panel, and the London Mayor's Office (City Hall) for additional guidance. The MPS has also commissioned the National Physical Laboratory (NPL) to undertake a ground-breaking equitability study on the use of LFR technology in an operational context to further build on the high levels of diligence already conducted on the FR algorithm.

4.10 The MPS has listened carefully to many parties with an interest in the use of LFR and has carefully considered what safeguards are necessary to support the use of LFR. Deployments must be carefully designed and have clear documented objectives. The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality. Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any concerns the public may have about how their human rights are engaged.

4.11 The AO must also be satisfied that LFR Operators involved with the Deployment are appropriately trained, briefed, and accountable. Also, that equipment will be used correctly, and that those involved in the Deployment mitigate against inappropriate responses to LFR system Alerts.

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

4.13 The MPS 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. The MPS will implement a robust governance process to review the effectiveness and impact of LFR Deployments on an ongoing basis. The MPS 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 London communities as part of an ongoing process.

4.14 This document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

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 The MPS will:-

a) use overt LFR technology in a responsible way to locate people in accordance with the MPS's common law policing powers. This includes targeting those wanted by the courts, those who pose a risk of harm and those wanted for criminal offences. The MPS will focus on its policing priorities. These include tackling serious crimes, with a particular regard to knife and gun crime, child sexual exploitation, violence against women and girls, and terrorism. The MPS will actively target the criminals, serious crime groups and those committing crimes which are regarded as having a serious impact on local communities and LFR's ability to more precisely disrupt criminality, reduce harm to the public and increase public safety; *and*

b) strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep London safe for everyone; *and*

c) build public trust and confidence in the development, management and use of LFR by taking account of privacy concerns and maximising transparency; *and*

d) 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; *and*

e) ensure that the Deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework (see the MPS LFR SOP and MPS LFR Legal Mandate for a schematic of this framework); *and*

f) transparently identify, manage and mitigate reputational and organisational risk to the MPS; *and*

g) be recognised as a responsible, exemplary and ethical organisation.

Operational Objectives

5.3 The MPS will:-

a) use LFR technology to enable the MPS to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities; *and*

b) adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight is active and involved, with the officer retaining full control and making the decision on whether or not to take action; *and*

c) engage with and provide reassurance to communities, listening and responding to concerns; *and*

d) continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

Technological Objectives

5.4 The MPS will:-

a) ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; *and*

b) provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other serious offences; *and*

c) look to technology improvements whilst keeping the MPS model under review.

Use Case

5.5 This document relates to the use of LFR in an overt capacity to locate those on a Watchlist to help the MPS protect the public. This reflects the MPS strategic intentions to place a focus on targeting criminals and serious organised crime, dismantling the organised crime groups and reducing the risk of harm facing the general public across London. From a MPS perspective, the following examples can be seen as factors that will currently inform an AO's judgment as to what constitutes 'serious crime' for the purposes of an LFR Deployment.

a) The nature of the offending being targeted – in terms of (i) potential sentences for the crime types sought (ii) the use of violence and/or the level of coercion involved in the offending, and (iii) the involvement of weapons.

b) The importance of addressing the crime issue – this includes (i) the level of organisation seen in relation to the crime types targeted (ii) the impact the crime is having or could be reasonably be expected to have on the local community, and (iii) the threat posed to public safety.

c) Examples where the seriousness of certain offences have been recognised - particularly where there are identified public protection considerations – this may include (i) the Serious Crime Act 2015, (ii) Schedule 15 of the Criminal justice Act 2003 and (iii) Schedules 3 and 5 of the Sexual Offences Act 2003.

5.6 The above factors are not exhaustive in making a determination as to what constitutes a serious crime given that all LFR Deployments are intelligence-led and reflect current MPS policing priorities and objectives. Within the parameters of the MPS LFR Documents, it remains for the AO to be satisfied that targeting people wanted for any particular crime type is lawful, necessary and proportionate in the circumstances and in line with this MPS LFR Policy.

5.7 The MPS will keep the use of LFR under review to ensure LFR continues to be used as an effective crime-fighting tool.

5.8 LFR helps the MPS use its resources more precisely and efficiently. The MPS considers that LFR is better than humans at recognising persons from a dataset and quickly linking a match, whilst providing information that indicated why they may be of interest to the MPS.

5.9 The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies.

5.10 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 the MPS 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 MPS LFR Documents.

5.11 Given that LFR requires a member of MPS personnel to review every Alert in real-time for a decision as to whether any further action is required, the MPS will always deploy LFR in a way that is operationally effective and allows the MPS to act on any Alerts as they are generated. LFR will not be used indiscriminately.

6 Overview of LFR Deployment Processes

End-to-End Process

6.1 A high level summary of end-to-end process of a stand-alone LFR Deployment can be found annexed to this MPS LFR Policy and the MPS LFR SOP. The MPS LFR SOP also provides a greater level of detail about the processes involved in the Deployment of LFR by the MPS.

The technical operation of LFR

6.2 The technical operation of LFR can be summarised in six stages as follows:

Stage	Action
1	**Compiling or using an existing database of images**
	The LFR system requires a Watchlist of reference images, against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the facial features associated with their subjects are extracted and expressed as numerical values.
2	**Facial image acquisition**
	A camera takes digital pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition and using it as a live feed. The siting of the cameras, and therefore the LFR Deployment location, is important to the lawful use of LFR.
3	**Face detection**
	Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.
4	**Feature extraction**
	Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template.
5	**Face comparison**
	The LFR software compares the biometric template with those held on the Watchlist.
6	**Matching**
	When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A Threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the Alerts and make a decision as to whether any further action is required. In this way, the LFR system works to assist police personnel to make identifications, rather than acting as an autonomous machine-based process devoid of user input

Key Points

a) 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;

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

c) 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;

d) The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.

e) 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.

f) The biometric data of those who do not generate an Alert is automatically and permanently deleted.

Policing LFR Deployments Effectively

6.3 There must be sufficient appropriately trained resource deployed so as to be able to respond to Alerts. This is important in order to ensure that the LFR system, and the data processed by it, is being effectively used.

6.4 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, Alert latency, and the probability of people from the Watchlist being observed by the camera (i.e occlusion) and their likely presence are all matters that must be taken into account when deciding what resources should be available.

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

7 Governance, Oversight and Impact Assessments

LPEP and MPS Stipulations

7.1 Following consultation with the independent London Policing Ethics Panel (LPEP), the following stipulations for the ethical deployment of LFR have been proposed and accepted by the MPS:-

a) The overall benefits to the public must be great enough to sufficiently compensate for the potential public distrust it may invoke;

b) It can be evidenced that the technology itself will not result in bringing unacceptable gender or racial bias into policing operations;

c) Each Deployment must be appropriately assessed and authorised, demonstrating both necessity and proportionality for a specific policing purpose – the MPS Form LFR 1 provides for this process;

d) LFR Operators are trained to understand the risks associated with use of the software, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions*;*

e) The MPS, seeking cooperation and support from MOPAC (Mayor's Office for Policing and Crime), 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, whilst taking into account guidance from the Biometric and Surveillance Camera Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

Governance Framework

7.2 MPS LFR Documents address the stipulations detailed above. Governance and operational oversight of the use of the technology is approached in three stages, as follows:-

Stage 1: Pre-Deployment;

Stage 2: Operational Deployment*;*

Stage 3: Post-Deployment.

Pre-Deployment

7.3 Authority to Deploy LFR is an operational one, where the MPS Authorising Officer (AO) rank is set at a level of least Superintendent level. In exceptional cases of urgency, an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR.

7.4 Where an officer below the rank of Superintendent provides the authorisation, a Superintendent (or higher rank) must be informed as soon as practicable. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.

7.5 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an MPS officer of NPCC rank[1] (or police staff equivalent) must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-London issues are taken into account as much as possible. This affords NPCC officer (or police staff equivalent) the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

7.6 A number of specific MPS documents and records need to be completed in support of each Deployment. These are set out below:-

MPS LFR Deployment Specific Documents and Records	
Pre Deployment:	
LFR Application – MPS LFR Form 1, Part 1	Explains how the proposed use of LFR is based on an intelligence case. The 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 – MPS LFR Form 1, Part 2	The AO's written authority provides a decision making audit trail demonstrating how the AO has considered the legality, necessity and proportionality of the Deployment of LFR, the safeguards that apply to it and the alternatives that were considered but deemed to be less viable to realise the policing purpose. The document will also detail and/or confirm the MPS LFR Policy / MPS LFR SOP applies in relation to: • awareness raising measures prior to and during the Deployment such that it is not covert and the public can be aware LFR is in use; • how fair processing information will be made available in public spaces where LFR is being deployed and on police websites; • how individuals can exercise their rights under data protection law; • the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR Deployment; and • the arrangements that have been made to gather metrics to assess the benefits of the 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.

[1] NPCC –`NPCC rank' denotes an officer holding the rank of Commander or above.

MPS LFR Deployment Specific Documents and Records	
Assessments	These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Surveillance Camera Commissioner's Self-Assessment. These documents need to be considered by the AO when authoring a Deployment to ensure they are sufficient to address the issues arising from the proposed Deployment. The AO 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. The Gold Commander must ensure that the assessments remain under review after the AO's authority during the pre-planning process and then during the Deployment itself. The MPS Data Protection Officer is an integral part of ensuring compliance with data protection legislation and the completion of the DPIA and they should continue to be engaged as necessary.
Operational Risk Assessment	A documented assessment of specific operational risks associated with the Deployment of LFR including decisions taken regarding mitigation. The Gold Commander is to review, amend where required and adopt the Operational Risk Assessment to ensure that it aligns with their strategic intention for the Deployment as part of the pre-Deployment process.
During the Deployment:	
Deployment Logs	Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Gold and Silver Commanders, and LFR Operators.
Post-Deployment:	
Cancellation Report – MPS LFR Form 1, Part 3.	Records details of where and when LFR was Deployed, the circumstances that brought the use of LFR to a conclusion, what resources were used, relevant statistics and performance metrics, outcomes and summary of any issues following a post-deployment review.
MPS Deployment Record	The MPS Record of LFR Deployments includes key metrics from the Deployment that will be updated and made available to the public online.

7.7 A number of other specific MPS documents that will be relevant to each MPS LFR Deployment have been completed centrally. These are set out below:-

MPS LFR Documents and Records	
MPS Data Processing – Appropriate Policy Document	MPS policy on the processing of data pursuant to the Data Protecting Act 2018 relating to LFR.
MPS Legal Mandate	Outlines the legal considerations to be addressed in order to use LFR.
MPS Training Materials	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.
MPS Facial Recognition Technology: Understanding accuracy and demographic differences	Provides details on the MPS's diligence on the LFR algorithm used in terms of its statistical accuracy and demographic differential performance.

Operational Deployment

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

7.9 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 content:-

a) that the use of the LFR remains necessary and proportionate for the policing purposes identified in the Written Authority Document; *and*

b) that the safeguards identified in the written approval remain effective; *and*

c) that the level of officer support committed to the Deployment is enabling Alerts to be responded to effectively*; and*

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

7.10 Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples may 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 empowered and have absolute discretion to suspend or terminate the Deployment. Further details are provided within the LFR SOP.

7.11 In any event, the Gold Commander must conduct and record a review of the activity at suitable intervals during the Deployment. The timing and frequency of reviews is determined by the Gold Commander. A suitable period should be determined in the context of the Deployment. This review should address the continued legality, necessity and proportionality of the Deployment, as well as providing some analysis on LFR system performance and the Engagements undertaken.

Post-Deployment

7.12 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.

7.13 Each MPS LFR Form 1 provides for an authority cancellation, once no longer required. The LFR Cancellation Report is submitted to the AO (this may be the same person as the Gold Commander) to ensure that appropriate senior oversight is maintained. Such reports should typically be produced and submitted within 31 days. These will be periodically reviewed by the SRO and the MPS FR Technology Board to consider effectiveness and trend. This ensures the outcome of LFR Deployments are subject to evaluation, which in turn should feed into oversight and scrutiny processes.

7.14 Post-Deployment, the MPS must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with the MPS LFR documents. This includes 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, following the conclusion of the Deployment.

7.15 Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:-

a) personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*

b) personal data is retained in accordance with the MPS's complaints / conduct investigation policies.

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

a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or*

b) in accordance with the MPS's complaints / conduct investigation policies; and/or

c) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV

footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

8 Oversight Bodies and Regulatory Framework

8.1 Within the MPS, the senior internal oversight body for LFR is the MPS FR Technology Board, which in-turn answers to the MPS Management Board. In addition, MOPAC provide oversight and scrutiny while LPEP provide independent insight and guidance.

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

8.3 Further oversight opportunities arise in relation to the Information Commissioner's Office and the Biometrics and Surveillance Camera Commissioner. More detail on these roles:-

a) Surveillance Camera Commissioner (SCC); The role of the 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 or not the code requires amendment. On the 9th March 2021, the Home Office announced the appointment of a single Biometrics and Surveillance Camera Commissioner.

   Any MPS LFR system will need to comply with this Code and the twelve guiding principles. This document seeks to apply those principles.

   See www.gov.uk/government/organisations/surveillance-camera-commissioner;

b) Biometrics Commissioner (BC); The Commissioner is independent of Government and aims to keep the police use and retention of biometric data under review. The Commissioner makes decisions on applications made by the police to retain DNA profiles and fingerprints, and reviews national security determinations that are made or renewed by the Police in connection with the retention of DNA profiles and fingerprints. On the 9th March 2021, the Home Office announced the appointment of a single Biometrics and Surveillance Camera Commissioner.

   See: www.gov.uk/government/organisations/biometrics-commissioner;

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

   The Data Privacy Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

   See www.gov.uk/government/organisations/information-commissioners-office.

9 Public Engagement

9.1 Public engagement must be supported by the use of 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 providing information, including details of the Privacy Notice, should be distributed and feedback via e-mail 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. It is also helpful for officers to 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.

9.3 Key stakeholders, including MOPAC, may be invited to observe the planning and Deployment of LFR.

In Advance of Deployments

9.4 In advance of Deployments ensure that:-

a) LFR Deployments are, where possible without undermining the objectives for the Deployment, prior notified to the public using MPS websites and other appropriate communication channels (including social media) – such notifications will give a purpose for the Deployment (for example, to primarily locate those wanted for violent and other serious offences and those wanted by the courts)[2]; *and*

b) LFR awareness raising measures (e.g. signs and/or leaflets) are prepared to support LFR Deployment in line with the MPS LFR SOP; *and*

c) literature is prepared for persons who may be Engaged (to include information outlined within a privacy notice); *and*

d) 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[3]; *and*

e) external engagement is considered in discussion with the MPS LFR team. It may be appropriate to pursue engagement opportunities with a number of stakeholders, including MOPAC, local authorities, and public consultative or ethical review bodies. It is

[2] Consideration should be given providing a purpose for the Deployment after the event if it was not feasible to give prior notification of the Deployment's purpose.

[3] The use of a section 60AA power is limited to the removal of anything that conceals a person's identity as opposed to providing specific powers in relation to the use of LFR to locate someone.

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 ensure that:-

a) awareness raising measures are used in line with the MPS 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; *and*

b) notices with a brief explanation and reference to the MPS website are available to hand out to the public on request; *and*

c) literature is offered to persons Engaged by officers in accordance with the policy referred to above.

After Deployments

9.6 After Deployments ensure that:-

a) 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 MPS website in line with the completion of the MPS LFR Form 1. Care must be taken to ensure that no personal data is published; *and*

b) external engagement is considered in discussion with the MPS LFR team. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders, including MOPAC, 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. The best images are those that follow a custody or passport style image that conforms to the NPIA '*Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)*'. Further detail is included within the embedded PDF:

NPIA Standard Still Digital Images.pdf

10.2 Where multiple images of a subject are available, consideration should be given to including these in the Watchlist where it is advised that they will improve the likelihood of locating those of interest to the MPS.

Compiling the Watchlist

10.3 The MPS Legal Mandate and other MPS LFR Documents provide commentary on the legal and MPS policy considerations relevant to compiling a Watchlist in a lawful way This means that we ensure we hold the Watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes. It helps ensure the public are informed as to the grounds needed to place an image on a Watchlist, and what considerations the MPS undertake in doing so.

10.4 Key points include the purposes for which an image may be added to the Watchlist, ensuring the Watchlist is limited to the size needed to meet the policing purposes identified, that particular privacy considerations may attach to non-police originated images and the need to take reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. The MPS LFR SOP provides practical direction on how to follow the MPS LFR Documents, including the MPS Legal Mandate.

10.5 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 system.

10.6 As explained in section 4 (LFR Overview), Watchlist composition is normally restricted to individuals suspected 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. How great that likelihood needs to be will vary between cases for inclusion, but in any case should be considered against a number of factors. This means that 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 London they might be found. Factors for consideration in this respect include:-

a) Severity of offence in question; this will often be relevant to the level of urgency associated with locating and arresting an individual. Many individuals change their

behaviour, including the places they reside and frequent when they know that they are wanted for a serious offence;

b) Risk; The level of risk associated with an individual or the offence type sought, whether that risk is to the public or themselves;

c) Crime trends; Where there is evidence of wider organisation, repeat offending, methodologies being replicated or numbers are exponentially rising. Emerging or specific crime issues may require a broader approach in order to reassure the public and increase community safety through the use of a precision crime-fighting tactic in order to effectively respond to crime issues.

d) Deployment location; the specific characteristics of the Deployment location may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the Watchlist. For example, areas around transport hubs have a lot of people transiting from place to place and other areas of London have 'pull factors' that make it likely that people from across London and beyond may frequent that area.

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 The MPS LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

Addressing Disproportionality

10.9 In normal operational circumstances, the MPS does not create or retain a breakdown of race, gender or any other protected characteristic[4] of persons on a Watchlist. This mirrors the approach taken with the majority of policing tools used by the MPS.

10.10 The Deployment of LFR is informed by the MPS Understanding Accuracy and Bias document and driven by MPS policing priorities, intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose that determines the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, there are prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.

10.11 The routine retention of data relating to protected characteristics would mean the MPS holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a Watchlist.

10.12 The MPS recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. The MPS use of LFR is informed by the MPS Facial Recognition

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

Technology: Understanding accuracy and demographic differences document. Moreover, to ensure system functionality, regular tests are carried out using police officers and staff volunteers who are `seeded' into a `Blue Watchlist'. The volunteers walk through the Zone of Recognition at the start of a Deployment to measure the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated.

10.13 The MPS also carries out scientific bias testing of the LFR system when necessary – such tests, including with the NPL have been documented in the MPS Facial Recognition Technology: Understanding accuracy and demographic differences document. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

10.14 The MPS also has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. For example, being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:-

a) those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and Environmental Factors throughout the Deployment. Should concerns arise that the LFR system is not performing correctly, the Silver commander will halt the Deployment where necessary; *and*

b) for the purpose of facilitating post-Deployment reviews, Alerts are retained for up to 31 days. It 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 the Silver and Gold Commanders during the Deployment; *and*

c) in the event post-Deployment reviews identify an area of concern, the MPS may undertake further bias testing where this appears necessary.

11 Guidelines for LFR

11.1 A new international standard (ISO IEC 30137-1: `Use of biometrics with video surveillance systems, Part 1: System design and specification)' was published in May 2019. See www.iso.org/standard/64935.html.

11.2 ISO IEC 30137-1 provides additional detail covering technical aspects of specifying and implementing a facial recognition system for use with video cameras, including camera selection and placement, adjustment of detection and matching Thresholds, Watchlist management, and the role of the LFR Operator. It is strongly recommended that forces considering the use of LFR use the guidance to supplement the technical overview provided here. The MPS has done this.

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

11.4 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 document. Directly relevant components include:-

a) the Cameras, including cabling, and their placement; *and*

b) the environment in which the cameras operate; *and*

c) the database of reference images and associated meta data, often referred to as the Watchlist; *and*

d) the facial recognition software that detects faces in the footage, converts the facial images into Templates, compares these against the Watchlist and provides information on the results of the comparison (generally in the form of an Alert or a numerical score) to an LFR Operator; *and*

e) the LFR Operator and LFR Engagement Officer who assess Alerts and determine the appropriate course of action*; and*

f) 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 50 and 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED). The FR vendor should advise on specific requirements for their system.

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 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 use of an `attractor' to direct a subject's gaze towards the camera may help to obtain better quality images.

12.8 Detection and processing of faces is an intensive task for a computer system. The supplier of LFR software should provide guidance on hardware requirements and the number of faces that can be simultaneously processed from within a single frame. If the system is set to process too many faces, this will potentially result in delays to the LFR system response. It may also result in missed Alerts due to 'dropped frames' where the software skips some of the video footage in an attempt to catch up.

13 Key Performance Metrics

13.1 This section covers the key performance metrics which should be gathered when deploying LFR. There are two key metrics that determine the 'accuracy' of an LFR system. These are the minimum requirements and so additional metric or indicators may well be relevant and suitable for collation and analysis (these can be specified by the AO).

True Recognition Rate (TRR)

13.2 This is also referred to as the True Positive Identification Rate.

13.3 The TRR is the total number of times an individual(s) on a Watchlist known to have passed through the Zone of Recognition and correctly generate an Alert, as a proportion of the total number of times the individuals who pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR application or not.

13.4 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 LFR systems (and vendors) must not focus so closely on maximising this metric, as it may increase the False Alert Rate to an extent that is not possible to manage the number of false alerts.

False Alert Rate (FAR)

13.5 This is also referred to as the False Positive Identification Rate.

13.6 The FAR 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.

13.7 All of the TRR and FAR metrics should be recorded and reported to the SRO. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e., less than 1 in 1000) and for the MPS, this is the standard endorsed by the SRO. It should be noted that the number of false alerts generated is greatly affected by the number of subjects processed by the LFR system, and to a lesser extent, the size of the Watchlist.

13.8 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 True alerts, whilst keeping the number of False Alerts within the 1 in 1000 levels as determined by the MPS's SRO.

Recognition Time (RT)

13.9 A third important metric is the Recognition Time. This is the average time taken between a subject on the Watchlist passing before a camera and the generation of an alert. 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 to assess the Alert to then make a final decision on whether to Engage or not.

13.10 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.

14 LFR Policy Summary

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

14.2 It is strongly advised that officers and staff adhere to the document, as this will help ensure that the MPS 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.

14.3 This document will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. By exception, if a decision is contemplated which would be outside of the MPS LFR Documents, any such decisions should be supported by legal advice (this being particularly relevant given this documents are published to ensure the use of LFR is accessible and foreseeable to the public). Such decisions will be rare and would typically arise where the circumstances move beyond those contemplated by this policy and give rise to a risk to the public and/or to the police. Any such decision must be fully documented and supported by a detailed rationale. Such decisions will be cited to the LFR SRO for review. This ensures that relevant decision-making features are subject to a debrief and evaluation processes.

15 Acronyms used in LFR

AFR	Assisted Facial Recognition (also sometimes referred to as Automated Facial Recognition). See paragraph 1.5.
AWC	Additional Watchlist Category
AO	Authorising Officer
BC	Biometrics Commissioner
CCTV	Closed Circuit Television
CFRS	Covert Real-Time Facial Recognition Surveillance
CIA	Community Impact Assessment
COIFRS	Covert Operator Initiated Facial Recognition Surveillance
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
IED	Inter-Eye Distance
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LPEP	London Policing Ethics Panel
LFR	Live Facial Recognition
MOPAC	Mayor's Office for Policing And Crime
MOPI	Management Of Police Information
MPS	Metropolitan Police Service

AFR	Assisted Facial Recognition (also sometimes referred to as Automated Facial Recognition). See paragraph 1.5.
NPCC	National Police Chiefs' Council
NPIA	National Police Improvement Agency (now the College of Policing)
NPL	National Physical Laboratory
OIFR	Operator-Initiated Facial Recognition
PWC	Primary Watchlist Category
RFR	Retrospective Facial Recognition
RT	Recognition Time
SCC	Surveillance Camera Commissioner
SCCSA	Surveillance Camera Commissioner's Self-Assessment
SOP	Standard Operating Procedure
SRO	Senior Responsible Officer
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition

16 Government Protective Marking Scheme

Protective marking:	Official
Publication scheme Y/N:	No
Title:	MPS LFR Policy Document
Version:	Version 3.0
Summary:	Guidance for the MPS Deployment of Live Facial Recognition Technology.
Branch:	MPS LFR
Review date:	20th March 2024