Surrey & Sussex

Policy Document for the Overt Deployment of Live Facial Recognition (LFR) Technology

Protective marking:	Official - Sensitive
Publication scheme Y/N:	No
Title:	Policy document for the overt deployment of Live facial recognition (LFR) technology
Version:	Version 1.1
Summary:	Guidance for SY/SX Deployment of Live Facial Recognition Technology.
Department:	Digital Services Division
Review date:	01/12/2025

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	02.05.2025	Project Lead	Ch. Insp. [redacted]	Initial Draft
0.2	02.06.2025	Programme Director	Det. Ch. Sup. [redacted]	First Review
0.3	17.09.2025	Project Lead	Ch. Insp [redacted]	Minor Amendments
1.0	10.10.2025	SRO	ACC [redacted]	No Amendments
1.1	10/11/2025	Programme Director	Det. Ch. Sup. [redacted]	Minor Amendments

Contents

Terms & Definitions: Capitalised terms used within this LFR Guidance Document shall have the meaning given to them in section 2 of this document unless otherwise defined.

1. Introduction, Aim and Scope

Introduction

1.1 Live Facial Recognition (LFR) is used by Surrey/Sussex (SY/SX) Police as a real-time deployment of facial recognition technology, which compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist, in order to locate persons of interest by generating an alert when a possible match is found. More detail about how LFR works and how SY/SX uses it can be found in section 3 (LFR Overview) and on the College of Policing website, https://www.college.police.uk/app/live-facial-recognition.

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

1.3 SY/SX is also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics and Surveillance Camera Commissioner and has participated in the development of national guidance, a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).

1.4 LFR is used by SY/SX purely in an overt capacity.

Aim & Scope

1.5 This guidance aims to: -

a) Provide SY/SX personnel and members of the public with information about SY/SX's present strategic, operational and technology objectives for the overt use of LFR, such that it enables SY/SX to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives)

b) Provide SY/SX personnel with guidance on the Deployment of overt LFR technology by SY/SX in spaces accessible to the public to meet SY/SX's objectives for LFR

c) Establish the governance structure for the Deployment of LFR, ensuring that SY/SX use of LFR is appropriately governed and legally compliant

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

Not in Scope

1.6 There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR), which relates to non-real time searching of images against a database. Also, not in scope is Operator Initiated Facial Recognition (OIFR) where an officer takes a

picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis.

1.7 In summary, this guidance does not extend to:

a) Manually instigated facial recognition for retrospective searching of video / still images

b) Human initiated facial search submitted from a mobile device in near real-time

c) Any SY/SX use of third-party LFR 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 guidance

d) The legal framework that is applicable to SY/SX's use of LFR – this is separately detailed within SY/SX's Legal Mandate document.

Additional Documents

1.8 Several documents are available to supplement this guidance, and these include but are not limited to, the:

e) SY/SX LFR Standard Operating Procedure (SOP)

f) SY/SX LFR Data Protection Impact Assessment (DPIA)

g) SY/SX LFR Legal Mandate

h) SY/SX LFR Appropriate Policy Documents

i) SY/SX LFR Equality Impact Assessment

j) SY/SX LFR Training Documents and User Guides.

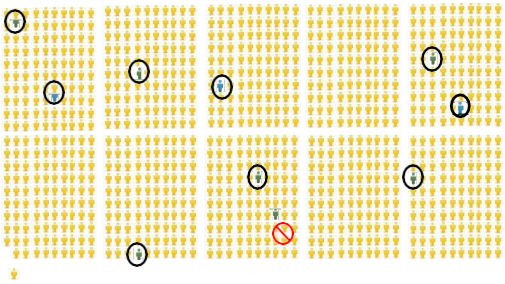
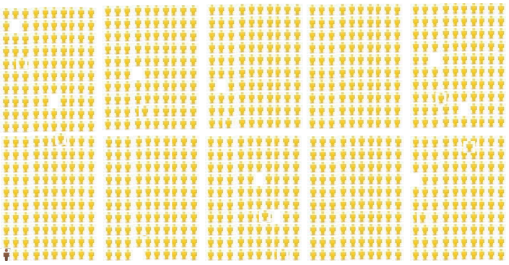
2. Terminology

2.1 Within SY/SX and throughout SY/SX LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition:

Adjudication	A human assessment of an alert generated by the Live Facial Recognition (LFR) application 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.
Administrator	A specially trained person who has access rights to the LFR application to optimise and maintain its operational capability.

Alert	An Alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the Watchlist and returns a comparison Similarity Score above the Threshold setting.
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 *(fig.1):*

(fig.1)

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

Authorising Officer (AO)	The Authorising Officer provides the authority for LFR to be used. LFR may not be used without this authorisation
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 specific 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 Watchlist comprising 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	The image of a person added to the Watchlist and the result of an Alert.
Confirmed False Alert	Following an Engagement, it is determined that the Engaged individual was matched by the technology but is not the person sought. This would not be treated as a true match, and the persons details would be deleted.
Confirmed True Alert	Following an engagement, it has been determined that the engaged individual is the person sought on from the Watchlist.
Deployment	Use of an LFR as authorised by an AO to locate those on an LFR Watchlist.
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, 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 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).
False Alert Rate ***This is also referred to as 'False Positive Identification 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.
False Negative	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 may 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).
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 sought by SY/SX Police by generating an alert when a possible match is found.
LFR Engagement Officer	An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR Deployment.
LFR Operator	An officer or staff member whose primary role is operating the LFR system. They will consider Alerts and, via the adjudication process, will assist LFR Engagement Officers in deciding whether an alert should be actioned.
Possible Match	A person returned because of the Probe and Candidate Image being of sufficient similarity above the threshold. Where the Similarity Score exceeds the Threshold Setting, an alert will generate for consideration by the LFR Operator

Probe Image	A facial image that is used to create a biometric template, which is compared 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 either generates an Alert or decides there is no match
Retrospective Facial Recognition **(RFR)**	A post-event use of Facial Recognition Technology, which compares still images of faces of unknown Subjects against an Image Reference 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 template and Candidate template, with a higher score indicating greater points of similarity.
Subject Factor	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	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 correct Possible Matches for Adjudication by the LFR Operator, whilst keeping the False Alert Rate to an acceptable level.

True Alert	A True Alert is the term used when it is determined by a human operator that the potential match presented by the LFR system is correct in that the Probe Image is the same as the candidate image in the watchlist.
True Recognition Rate ***This is also referred to as the 'True Positive Identification 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 t times those individuals passed through the Zone of Recognition during that deployment (regardless of whether an Alert is generated). By way of an example, the rate would be 90% if 10 people on the Watchlist each pass the LFR system a single time amongst a much larger crowd, and that led to the generation of 9 alerts relating to 9 of those 10 people. Alternatively, the rate would also be 90% if the total number of people on a watch list was 5, and all 5 of those persons went through the Zone of Recognition twice each with 2 alerts being generate for each of 4 of those people and only a single alert being generated for the last fifth member of the watchlist.
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 (whilst taking account of the Force's public and legal obligations and the need to act in accordance with the principles of necessity and proportionality).
Watchlist	A set of known Candidate images against which a Probe image is searched. The Watchlist is normally a subset of a much larger collection of images (from the Image Reference Database) and will have been created specifically for the LFR 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 facial recognition. Signage notifying the public that there is an LFR operation taking place will be set out wider than the zone of recognition to allow the public the option to not enter the zone.

3. LFR Overview

LFR in a Law Enforcement Context

3.1 Live Facial Recognition (LFR) is used by SY/SX, it compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist to locate people who are:

a) wanted by the courts

b) suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence, or where there are reasonable grounds to suspect an individual depicted to be committing an offence

c) subject to bail conditions, court order or other restriction that would be breached if they were at the location of the Zone of Recognition at the time of the deployment

d) missing persons deemed at increased risk of harm

e) presenting a real risk of harm to themselves or significant risk of harm to others

f) a victim of an offence or a person who the police have reasonable grounds to suspect would have significant information of importance and relevance to progress an investigation.

3.2 LFR is a tool designed to help Police locate specific persons. It does this by monitoring facial images of people who pass within a Zone of Recognition. Images from specially placed cameras focused on that zone are processed and searched against a specific Watchlist of Candidate Images of people who the Police wish to locate.

3.3 LFR works by analysing key facial features to generate a mathematical representation of them (often known as a biometric template). This representation is then compared against known faces in a database that has been compiled for that specific deployment (the watchlist) to identify Possible Matches against specific persons of interest. Where the LFR application identifies a Possible Match, the LFR system flags an Alert to a trained member of SY/SX personnel who then decides as to whether any further action is required. In this way, the LFR application works to assist SY/SX personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

LFR and SY/SX

3.4 SY/SX believes that LFR is a valuable precision policing tool that helps SY/SX 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 as well as those relating to the wider safeguarding role of SY/SX.

3.5 The following are some illustrative examples where LFR may assist SY/SX with its policing purposes:

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

b) Preventing people who may cause harm and who are prohibited from entering an area (e.g. under football banning orders).

c) Supporting the identification of people about whom there is intelligence and a reasonable basis to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons, sex offenders etc.).

d) Supporting the use of targeted preventative policing tactics in areas where

intelligence suggests violent 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.

3.6 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. SY/SX is conscious that the use of LFR has been the subject of much debate. Areas of scrutiny relate to:

a) the privacy intrusion and the impact on wider civil liberties,

b) instances of false reporting relating to the accuracy of LFR,

c) the potential for wide-scale monitoring using LFR

d) the possibility for automated decision making because of LFR processing.

3.7 It is therefore incumbent on SY/SX 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 using LFR.

3.8 In seeking to address other potential concerns, SY/SX will be using technology that has been subject to academic research led by the National Physics Laboratory (NPL).

3.9 SY/SX 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. Each Deployment must be carefully designed and have clearly 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 any concerns the public may have with regards to how their human rights are engaged.

3.10 The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the Deployment are appropriately trained, briefed, accountable and that equipment will be used correctly, and that those involved in the deployment mitigate against inappropriate responses to LFR application alerts.

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

3.12 SY/SX 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. SY/SX will implement a robust governance process to review the effectiveness and impact of LFR deployments on an ongoing basis. SY/SX 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 SY/SX communities

as part of an ongoing process.

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

4. Strategic Intention, Objectives and Use Case

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

Strategic Intentions

4.2 SY/SX will:

a) Use overt LFR technology in a responsible way to locate offenders in accordance with SY/SX's common law policing powers. This includes targeting those wanted for criminal offences, those who pose a significant risk of harm and those wanted by the courts.

b) Comply with the common law and all statutory safeguards in delivering its policing operational duties and relies on the common law to discharge several of its duties. LFR can assist with SY/SX's duties to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security. This includes targeting those wanted for offences. It also includes using LFR technology to protect the public, reduce crime and help safeguard vulnerable persons.

c) Strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep SY/SX safe in a way that is both necessary and proportionate having regard to the rights of those whose data is processed.

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

e) 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 alongside a process of continual review of both documentation and process.

f) Ensure that the Deployment of LFR follows all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and the relevant SY/SX LFR documents.

g) Transparently identify, manage and mitigate reputational and organisational risk to SY/SX

h) Recognise as a progressive, responsible and ethical organisation.

Operational Objectives

4.3 SY/SX will:

a) Use LFR technology to enable SY/SX to discharge its common law and other policing powers. This includes the need to tackle our foremost operational priorities.

b) Adopt a robust and proportionate approach in engaging and pursuing individuals following a true alert that identifies a match using both LFR input and human decision-making. Officer oversight is active and involved, with the officer retaining full control by making the decision on whether to act in each case.

c) Engage with and provide reassurance to communities, listening and responding to concerns

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

Technological Objectives

4.4 SY/SX will:

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

b) Provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic and considering the relevant legal obligations.

Use of LFR

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

4.6 LFR helps SY/SX use its resources more efficiently. SY/SX considers that LFR is better than humans at recognising persons from a large dataset (generally hundreds to low thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to SY/SX.

4.7 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. (It is acknowledged that considerations regard data protection should not be considered as an absolute barrier to information sharing). Additionally LFR presents a method that provides enhanced privacy features over other alternative methods of location (whether this be because information does not need to be shared publicly or externally with third parties, or because large number of officers do not need to be provided with identifying personal data of

persons in order to help them locate specific persons (and so the associated accidental disclosure risks are also avoided).

4.8 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 SY/SX in discharging its operational duties in a proportionate and compliant manner. 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 SY/SX LFR Documents.

4.9 Deployment of LFR will largely fall into one of three use cases. These are identified as:

a) **Proactive Deployments**: These are routine deployments of LFR to locations within the SY/SX area. These deployments will be based on information, intelligence and crime data for those areas, including increases in types of crime and persistence of crime occurring at significant volumes at a given location.

These deployments will be focused on locations and access routes where LFR will provide the most benefit in discharging the operational duties of SY/SX. Watchlists will be linked to the purposes of the deployment and there must be a reasonable suspicion that all subjects included in watchlists may attend at the deployment location.

b) **Event Deployments**: These deployments are in response to specific events which are expected to attract increased public attendance to an identified location. These deployments will support policing operations to ensure the safety of the public and the protection of critical infrastructure at the location. This will also include transport hubs and routes that can be identified as supporting attendance to the specified event.

An example of this would be a concert/ festival held at a rural location (which itself would not normally attract attendance from members of the public).

Watchlists will be compiled based upon the location and nature of the event, but there must be a reasonable suspicion that all subjects included in any watchlist may attend at the deployment location.

c) **Incident/ Intelligence specific Deployments**: These deployments will be in response to a specific incident or in response to specific intelligence. The watchlists for these deployments will cater to the geographical location of the deployment and include individuals based on the specific needs of the incident response or intelligence.

An example of this would be deployment of LFR to a location where disorder has recently occurred, and intelligence exists that the disorder may continue between identified individuals who have yet to be located. There must be a reasonable suspicion that all subjects included in any watchlist may attend at the Deployment location.

4.10 Given that LFR requires a member of SY/SX personnel to review every alert in real-time for a decision as to whether any further action is required, SY/SX will always deploy LFR in a way that is operationally effective and allows SY/SX to act on any alerts as they are generated. LFR will not be used indiscriminately, disproportionately or otherwise in a non-compliant manner.

5. Overview of LFR Deployment Processes

End-to-End Process

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

a) LFR law enforcement purpose identified, safeguards considered, Deployment authorised, and Watchlist selected.

b) Notification of Deployment, and signage deployed.

c) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist.

d) If a Possible Match is found in a Watchlist, the LFR application generates an alert and both the detected face from the video and the possible match image from the watchlist are presented to the LFR Operator / LFR Engagement Officer for human review. If no match is found, the detected face is deleted automatically and immediately.

e) The LFR Operator / LFR Engagement Officer will consider the alert, noting the system, subject and environmental factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is engaged.

f) Cancellation of authority for the LFR Deployment and post-deployment evaluation.

5.2 SY/SX LFR SOP provides a greater level of detail about the processes involved in the deployment of LFR by SY/SX.

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. Images from the live feed are processed immediately and momentarily. Where no match is detected the live feed images and

associated data are deleted and not further processed.

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 to ensure the minimum requirements of the relevant policies are met.

d) The inclusion of persons on a watchlist needs to be justified based on the principles of necessity and proportionality in line with the LFR documentation and all applicable legal obligations.

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 operationally less effective and not provide value for public money.

Policing LFR Deployments Effectively

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

5.4 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of false negatives, false alerts, recognition time, and the probability of people from the watchlist being observed by the camera and their likely presence are all matters that must be considered when deciding what resources should be available.

5.5 It is also vital that SY/SX is transparent in its use of LFR under this guidance. As well as using signage that ensures individuals are able to take action to prevent their personal data being processed, the provision of sufficient policing resource will also allow officers to answer any questions that the public may have.

6. Governance, Oversight and impact assessments

6.1 Following consultation, the following stipulations have been proposed and accepted by SY/SX:

a) The overall benefits to the public of deploying LFR must be balanced against public's confidence of our use of LFR technology.

b) Evidenced will be published that confirms the technology itself will not result in unacceptable gender or racial accuracy variance into policing operations.

c) Each deployment must be appropriately assessed and authorised,

demonstrating in writing why each specific deployment is both necessary and proportionate for a specific policing purpose or purposes.

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

e) SY/SX, 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 considering guidance from the Surveillance Camera and Biometric Commissioner, the ICO and others. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

Governance Framework

6.2 SY/SX LFR documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:

a) Pre-Deployment.

b) Operational Deployment.

c) Post-Deployment.

Pre-Deployment

6.3 Authority to Deploy LFR is an operational one, where SY/SX Authorising Officer (AO) rank is set at Superintendent. In exceptional cases of urgency, the forces Gold Commander for that period may authorise the deployment of LFR.

6.4 Prior to AO authorisation and the Deployment of LFR in public spaces, several documents must be completed. The documentation should be reviewed to ensure it is accurate, and a record made of that is, or isn't. Any changes will need to be recorded before the documentation is finalised and then relied on for a new deployment and an SY/SX 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 to expose the proposed deployment to an elevated level of strategic thinking, whereby issues are considered as much as possible. This affords NPCC the opportunity to scrutinise the deployment and to ask the AO to consider what mitigation is required to address concerns at hand.

6.5 Several specific SY/SX documents and records need to be completed in support of each Deployment. These are set out below:

SY/SX LFR Deployment Specific Documents and Records

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

LFR Application	Sets out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.
Written Authority Document	The AO's written authority provides a decision-making audit trail demonstrating compliance with the various requirements and following the details of all relevant policies. Setting out how the AO has considered the legality, necessity and proportionality of the Deployment of LFR, the safeguards that apply and the alternatives that were considered but deemed to be less viable to realise the policing purpose. The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained because of the LFR Deployment. The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.
LFR Deployment Record	Records details of where and when a Deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues along with recommendations as to mitigations or additional actions recommended for future deployments from a lesson learned perspective.
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 decision-maker when authoring a Deployment to ensure they are up to date, accurate and sufficient to address the issues arising from the proposed Deployment. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the deployment is compliant with all applicable requirements and in particular meets, the condition that the specifics of the proposed deployment in the circumstances envisaged is not only necessary but is also proportionate to the relevant policing purpose(s).
Deployment Logs	Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.

6.8 Several other specific SY/SX documents pertaining to each SY/SX LFR deployment have been completed centrally and will each be subject to regular periodic review.

The AO must consider each of these prior to a deployment and record whether they remain fit for purpose for the deployment or whether any changes need to be made. These central documents are set out below:

SY/SX LFR Documents and Records	
SY/SX Data Processing – Appropriate Policy Documents	SY/SX policy on the processing of data pursuant to the Data Protecting Act 2018 and UK General Data Protection Regulation relating to LFR.
SY/SX Legal Mandate	Outlines the legal considerations to be addressed to use LFR.
SY/SX 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.

Operational Deployment

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

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

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

b) The safeguards identified in the Written Authority Document remain effective

c) The level of officer support committed to the deployment is enabling alerts to be responded to effectively

d) The subject, system and environmental factors are such that the use of the LFR application remains effective and appropriate for realising the policing purpose identified in Written Authority Document.

6.11 Circumstances may arise that mean that there is a need to curtail, adjust 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, adjust or terminate the deployment. Further details are provided within the LFR SOP.

6.12 In any event the Silver 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 Silver 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 application performance and the engagements undertaken.

Post-Deployment

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

6.14 Each deployment should be subject of an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO (this may be the same person as the Silver Commander) to ensure that appropriately senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

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

6.16 Post-Deployment, SY/SX must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with SY/SX LFR documents, policy, procedure and legal obligations. This includes that:

a) The LFR system does not generate an alert that a person's biometric data is immediately automatically deleted

b) The data held on any 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.

6.17 The LFR system generates an alert, all personal data is deleted as soon as practicable and in any case within 24 hours.

6.18 All CCTV footage generated from LFR deployments is deleted within 24 hours, except where retained:

a) In accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996

b) In accordance with SY/SX's complaints / conduct investigation policies

c) Examples of when it may be retained passed 24hrs would be things such as, subject of Death or Serious injury as defined in the Police Reform Act, Critical/Major Incidents

7. Oversight Bodies and Regulatory Framework

7.1 Within SY/SX, the senior internal oversight body for LFR is currently the SY/SX Facial Recognition SRO Board. In addition, The SY/SX commissioner's office also provide an external oversight and scrutiny perspective.

7.2 SY/SX LFR Legal Mandate sets out the legal framework for SY/SX use of LFR technology, whilst SY/SX LFR Policy Document and SY/SX LFR SOP support implementation.[2]

7.3 Nationally, the `NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.

7.4 Further oversight opportunities may arise in relation to the `Joint National Biometric Strategic Board'. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the Information Commissioners Office, the Surveillance Camera Commissioner, and the Biometric Commissioner. More detail on these roles: -

a) Biometrics and Surveillance Camera Commissioner (BSCC)[3]; The role of the Biometrics and Surveillance Camera Commissioner is to:

- keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints.
- decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984)
- review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints
- provide reports to the Home Secretary about the carrying out of his functions
- encourage compliance with the Surveillance Camera Code of Practice
- review how the code is working
- provide advice to ministers on whether the code needs amending

The commissioner is independent of government. The commissioner has no enforcement or inspection powers regarding surveillance cameras and works with relevant authorities to make them aware of their duty to have regard to the code. See About us - Biometrics and Surveillance Camera Commissioner - GOV.UK (www.gov.uk)

b) Information Commissioner's Office (ICO)[4]; The ICO upholds information rights

[2] Live Facial Recognition | Surrey Police and Live Facial Recognition | Sussex Police
[3] Biometrics and Surveillance Camera Commissioner - GOV.UK
[4] Information Commissioner's Office

in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Protection 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/groups/chief-scientific-advisers

7.5 Further oversight will be provided by the forces 'Use of Force Committee'. This will provide internal scrutiny of LFR deployments and has independent representation to seek the public's view on the deployment of LFR. This committee has been chosen to provide this independence, and it will not form part of the discussion around use of force.

8. Public Engagement

8.1 Public engagement must be supported using online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of Deployments in an appropriate and effective manner taking account of the specific circumstances of the deployment. At and around the location of deployments, notices providing information, including details of the Privacy Notice, should be distributed and feedback via email should be sought. Consideration must be given to tailoring the information provided to ensure it is effective and fulfils its purpose in the context. For example, for deployments in areas where there are many individuals who speak a language other than English as their first language, consideration should be given to signage and notices being made bi-lingual. Equally where a deployment is likely to encounter significant numbers of persons with limited eyesight either due to age or disability, again consideration should be given to mitigations such as audio as well as printed information and increased font size material.

8.2 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. Information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.

8.3 Key stakeholders, including the PCC's Office, may be invited to observe the planning and deployment of LFR.

In Advance of Deployments

8.4 In advance of deployments ensure LFR business owners will ensure that:

a) LFR Deployments are notified to the public using SY/SX website at least 5

days before the deployment.

b) LFR awareness raising measures (e.g. signs and/or leaflets or other measures as appropriate) are prepared to support LFR Deployment in line with SY/SX LFR SOP

c) Inclusive Literature (and alternative media as necessary) is prepared for persons who may be engaged (to include information outlined within a privacy notice)

d) Officers are briefed on their powers and the limits thereof. It must be made clear that there is no power to require an individual's cooperation (or to force them) to be subject to LFR processing. Whilst there are powers relating to arrest and to compel the removal of items that conceal identity, they exist in contexts, and for purposes and do not explicitly extend to the compulsory application of LFR processing to an individual. For example, where 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, this may mean that if subject to LFR processing it is more likely a usable image will be captured. However, the overt nature of LFR which is based around the concept that individuals will always be able to choose whether or not to be subject to LFR processing, and the lack of an explicit coercive power means that even where items have been removed under the S.60AA power there is no guarantee such persons will choose to enter the zone of recognition; and

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

During Deployments

8.5 During Deployments ensure LFR business owners will ensure that:

a) awareness raising measures are used in line with the SY/SX 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 as well as for what purposes; and

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

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

After Deployments

8.6 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 SY/SX website and potentially social media to demonstrate the results. Care must be taken to ensure that no personal data is published unless it is compliant (as well as specifically that it is fair and necessary) to do so.

b) External engagement is considered in discussion with SY/SX LFR team. Again, it may be appropriate to pursue engagement opportunities with several stakeholders, including local authorities, local groups 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.

c) Engagement with representatives from the Information Commissioners Office and the Biometrics and Surveillance Commissioner will be ongoing.

9. Watchlist Considerations

Image Quality

9.1 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 the established model found in custody or passport style images. SY/SX will conform to the standard set by the Surveillance Camera Commissioner in the document 'Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales.' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

Compiling the Watchlist

9.2 SY/SX Legal Mandate provides commentary on the legal 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. The watchlist is specific for each deployment using assessed information that's held and reviewed on our crime management system.

9.3 Key points include ensuring the watchlist is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. SY/SX LFR SOP provides practical guidance on how to follow SY/SX LFR Documents, including SY/SX Legal Mandate.

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

9.5 As explained in section 3 (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, it should be considered against several 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 SY/SX 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) 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. Areas around transport hubs have a lot of people transiting from place to place. Similarly certain events such as sports matches will often draw both local and 'away' team support and so may justify inclusion of persons who are not normally proximate to that area normally but in this context, there is a real possibility of them being in that area at the proposed time and place of deployment.

Governing the Watchlist

9.6 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.

9.7 SY/SX 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

9.8 SY/SX does not create or retain a breakdown of race, gender or any other protected characteristic[5] of persons on a Watchlist. This mirrors the approach taken with most policing tools used by SY/SX. The exception here is for inclusion of under 18's and under 13's as per the application form.

9.9 The deployment of LFR is driven by SY/SX policing priorities and 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 realistic prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.

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

9.10 The routine retention of data relating to protected characteristics would mean SY/SX holding and processing data in circumstances where it does not have a policing need to do so. In essence, collecting and holding specific protected characteristics data would not alter the intelligence case or change the policing need to locate individuals placed on a watchlist. Consequently, such data is not and will not be routinely collected at deployments.

9.11 SY/SX 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. 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.

9.12 SY/SX also carries out academic equitability testing of the LFR system when necessary – such tests, including with the National Physical Laboratory have been documented. The necessity and frequency are determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

9.13 When equitability tests are conducted, no biometric data belonging to members of the public is retained for the purpose of the tests. As part of these tests, a human operator monitors and records perceived gender, ethnicity, age and any other relevant protected characteristics, of persons passing through the Zone of Recognition during an LFR Deployment.

9.14 SY/SX has several 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 are trained to 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

b) The purpose of facilitating post-deployment reviews, alerts are retained for up to 24 hours. 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 Silver and Gold during the deployment

c) In the event post-deployment reviews identify an area of concern, SY/SX may undertake further equitability testing where this appears necessary.

10. Testing Equitability

10.1 In August 2021 South Wales Police was awarded Home Office Science, Technology, Analysis & Research (STAR) funding to undertake testing of the accuracy and equitability of FRT in an operational environment for LFR, OIFR and

RFR.

10.2 In collaboration with the Metropolitan Police Service (MPS), this work was awarded to the National Physical Laboratory (NPL) at the end of 2021. The NPL is a prestigious world-leading centre of excellence that provides cutting-edge measurement science, engineering and technology to underpin prosperity and quality of life in the UK. To deliver on the objectives of the research, it was necessary to use LFR in the operational use cases of UK Policing. Data collection for the evaluation took place in July and August alongside five operational deployments of LFR, four in London and one in Cardiff.

10.3 A cohort of volunteers were selected to take part in the study who were of varying age, gender and race, the volunteers were seeded into the crowd passing the LFR System at each deployment to appear in the LFR video footage.

10.4 The data was then evaluated 'post event' with a balanced watchlist and mated facial photographs taken of the volunteers in a variety of settings to realistically replicate the use cases for LFR, RFR and OIFR.

10.5 The full results are presented in the National Physical Laboratory's commissioned report 'Facial Recognition Technology in Law Enforcement Equitability Study'.[6]

What does this study tell us about accuracy of SY/SX's FRT?

10.6 The NPL report gives us an impartial, scientifically underpinned, evidence-based robust analysis of the performance of SY/SX's FRT System in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.

10.7 In summarising LFR operational performance, NPL have provided performance figures for two different Watchlist sizes: (i) a Watchlist of 10,000 reference images, which is broadly in line with those used on the MPS' LFR operational deployments to date and (ii) a watchlist of 1000 reference images a size more typical for SY/SX LFR deployments.

10.8 The performance figures use industry standard measures; (i) True-Positive Identification Rate (TPIR) (also known as True Recognition Rate)– the rate of successful recognition when subjects on the Watchlist pass through the Zone of Recognition (ii) False-Positive Identification Rate (FPIR) (also known as False Alert Rate) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the Watchlist pass through the Zone of Recognition

10.9 The table below shows the results of combined data from all five deployments:

Watchlist size 10000			**Watchlist size 1000**		
Metric	**Threshold Setting**	**Result**	**Metric**	**Threshold Setting**	**Result**
TPIR	0.60	= 89 %	TPIR	0.60	= 89 %
FPIR	0.60	≈ 0.017 % (1 in 6000)	FPIR	0.60	≈ 0.002 % (1 in 60,000)

[6] frt-equitability-study_mar2023.pdf

Did the study find any differences in FRT?

10.10 In relation to LFR, NPL found that at a Threshold of 0.60, any differences in TPIR by gender, by race, or by race/gender combined were not statistically significant. This means that the evidence indicates that the systems performance in these conditions is not biased towards any race or gender. The study has shown that at Thresholds of 0.60, 0.62 and 0.64 the number of subjects with a false positive is very small and there is no statistically significant imbalance between demographics.

10.11 The study has shown that at a face match Threshold of 0.64 or higher there was no false positive identifications. Thus, at this Threshold the FPIR is identical for race, age and gender.

10.12 In relation to age, the NPL found that at a Threshold of 0.62 the observed differences in TPIR were not statistically significant. At a Threshold of 0.60, the observed variation in TPIR did show statistical significance with TPIR improving with subject age. This means that the system is slightly more likely to locate those sought as they age, but not more likely to inconvenience those of younger age, as the FPIR is found to be equitable between gender, race, and age. There is no statistically significant imbalance between demographics. In relation to trying to locate those of younger age, the NPL recognised.

" ..... the lower performance of the under 20s is therefore assessed to be due to both

demographic and environmental factors, these being a combination of subject age and as a result subject height, and crowdedness in the zone of recognition ....."

10.13 Where SY/SX is particularly seeking to locate those of younger age and whom maybe of a shorter stature, consideration should be given of how busy the area is. The risk that subjects may be shielded from the camera by a taller person walking in front of them and blocking the camera's view must be considered. Therefore, deployment locations and camera positioning should form part of the technical optimisation process.

10.14 Reflective of the need for continuous improvement, SY/SX will continue to monitor its FRT performance, in terms of both overall system accuracy and demographic differential performance going forward.

11. Design Guidelines for LFR

11.1 A new international standard (ISO IEC 30137-1:2024 `Use of biometrics with video surveillance systems, Part 1: System design and specification)' was published in May 2019. See ISO/IEC 30137-1:2024 - Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification.

11.2 ISO IEC 30137-1:2024 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. SY/SX has done this.

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

11.4 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 guidance. Directly relevant components include:

a) The cameras, including cabling and/ or network capability, and their placement

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

d) Facial recognition software that detects faces in the video feeds, 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

e) The LFR Operator and LFR Engagement Officer who assess alerts and determine the appropriate course of action

f) Sufficient officer resource available to support the deployment.

12. Cameras and Camera Placement

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

13. Key Performance Metrics

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

True Recognition Rate

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

13.3 This metric can only be generated by 'seeding' known subjects (for example

police officers or staff) into a ‘Blue Watchlist’ and measuring the number of times those subjects are present in the Zone of Recognition against the number of alerts generated. Users of FR systems (and vendors) must not focus so closely on maximising this metric, that they increase the false alert rate to inappropriate levels.

False Alert Rate FAR

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

13.5 All the TRR and FAR metrics should be recorded and reported. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the FAR is greatly affected by the number of subjects processed by the LFR application, and to a lesser extent, the size of the watchlist. This is a key reason why the number of persons included on the watchlist needs to be kept as small as possible, whilst still meeting operational objectives.

13.6 It should 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 to maximise the probability of returning correct possible matches, whilst keeping the number of false alerts to acceptable levels.

Recognition Time

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

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

14. LFR Guidance Summary

14.1 This guidance 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 guidance as this will help

ensure that SY/SX use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintain the trust and confidence of the public as well as our partners and other stakeholders.

14.3 It is recognised circumstances may arise where for valid reasons, a decision is taken that it is necessary to change things slightly outside of this guidance. This guidance will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are at odds with some aspects of this guidance, it is essential these decisions are fully documented, together with detailed rationale, and that the relevant decision-making features within debrief and evaluation processes.

15. Acronyms Used in LFR

AO	Authorising Officer
BC	Biometrics Commissioner
CCTV	Closed Circuit Television
CIA	Community Impact Assessment
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EIA	Equality Impact Assessment
FAR	False Alert Rate
FR	Facial Recognition
FoIA	Freedom of Information Act
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LFR	Live Facial Recognition
MOPI	Management of Police Information
SY/SX	Surrey/Sussex
NPCC	National Police Chiefs' Council
NPL	National Physics Laboratory

RT	Recognition Time
SCC	Surveillance Camera Commissioner
SCCSA	Surveillance Camera Commissioner's Self-Assessment
SOP	Standard Operating Procedure
SRO	Senior Ranking Officer
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition