Home Office

Immigration Enforcement Live Facial Recognition Policy Document

Direction for Immigration Enforcement (IE) use of overt Live Facial Recognition to locate person(s).

Version No: 1.0
Issue Date: Oct 2025

Document History

Issue Date	Version No	Produced By	Contents
23/10/25	1.0	M.WILKINSON	First version

Final Version Distributed to:

Name	Role
Gordon Summers	SRO

Table of Contents

1. Introduction, Aim and Scope

Introduction

1.1 Immigration Enforcement (IE), with Border Force and police partners, will run an overt, time-limited Live Facial Recognition (LFR) proof of concept (POC) at UK port in late 2025 focused on identifying and locating persons returning in breach of a Deportation Order (DO) for law enforcement purposes.

1.4 This IE LFR Policy Document provides IE personnel with direction on the overt use of LFR to locate persons returning in breach of a Deportation Order (DO) in a legally compliant and ethical manner to enable IE to achieve legitimate enforcement aims.

1.5 IE is cognisant of the views and ongoing considerations of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner. This document will be reviewed as new policy and guidance is published.

1.6 IE policy and guidance should be read having regard to the APP guidance on the use of LFR produced by the College of Policing.

Aim & Scope

1.7 This document aims to: -

- Provide IE personnel and members of the public with information about IE's present strategic, operational and technology objectives for the overt use of LFR to identify and locate those persons returning in breach of a Deportation Order, contributing to IE to achieving its enforcement aims.

- Provide IE personnel with direction on the construction of Watchlists and the implementation of overt LFR technology by IE in spaces accessible to the public to meet IE's Objectives for LFR; and

- Establish the governance structure for the implementation of LFR, ensuring that IE's use of LFR is appropriately governed and legally compliant; and

- Provide an overview of LFR and advise on practical issues to obtain the best performance from the LFR system.

1.6 IE will publish a suite of documents, to assist the public who may pass an LFR system and those who may be placed on a Watchlist to understand the standards to which IE, as a public body, operates. In doing so, IE 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.

Additional Documents

1.8 Several documents are available to supplement this document, and these include:

- Immigration Enforcement Standard Operating Procedure (SOP)

- Immigration Enforcement Data Protection Impact Assessment (DPIA)

- Immigration Enforcement Equality Impact Assessment (EIA)

- Immigration Enforcement Legal mandate

- Immigration Enforcement Policy documents

- Appropriate Policy Document: processing special categories and criminal convictions data under UK GDPR and Part 2 DPA (2018)

- Policy on sensitive processing for Law Enforcement Purposes, under Part 3 DPA (2018)

Terminology

1.9 The following terms and definitions apply in respect of LFR. These are in line with those used by other police forces and the College of Policing.

Adjudication

A human assessment of an alert generated by the LFR application by an LFR engagement officer (supported, as needed, by the LFR operator) to 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 factors, system factors and environmental factors

Administrator

A specially trained person who has access rights to the LFR application, in order to optimise and maintain its operational capability.

Alert

A notification generated by the LFR application when a facial image from the video stream, which is being compared against the watchlist, returns a comparison (similarity) score above the threshold.

True alert

When it is determined that the probe image (the image from the video stream) is the same as the candidate image in the watchlist.

Confirmed true alert

When, following engagement, it is determined that the engaged individual is the same as the person in the candidate image in the watchlist.

True recognition rate (TRR)

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

This is also called the **True Positive Identification Rate**. The TRR measures how often individuals on a Watchlist are correctly identified by LFR technology when passing through the Zone of Recognition, as a proportion of all

instances where individuals pass through or are processed. It is calculated by seeding known subjects into a Watchlist and comparing their presence with the number of alerts generated. Users and vendors should avoid focusing solely on maximizing this metric, as it can significantly increase unmanageable false alerts.

This is also referred to as the true positive identification rate.

False alert

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

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

Confirmed false alert

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

False alert rate (FAR)

The number of individuals who are not on the watchlist but generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition.

This is also referred to as false positive identification rate.

Application accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the true recognition rate and the false alert rate. This is further explained below. The example given has been simplified to demonstrate the concept. Note that the metrics have been calculated in accordance with the agreed scientific method, as set out by the International Organisation for Standardisation.

The TRR, or true positive identification rate, would be 90% if, after 10 people on the watchlist pass the LFR system, a correct alert is generated for 9 out of 10 of those people. As no alert was generated against one person in this example, there was one missed alert.

The FAR, or false positive identification rate, would be 0.1% if, for every 1,000 people that passed the LFR system, an alert was generated against one person who was not on the watchlist.

Authorising officer (AO)

The officer must be at least the rank of Grade 7 (G7), who provides the authority for LFR to be deployed.

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 that constitute biometric data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

Blue Watchlist

A watchlist comprising of known persons that can be used to test system performance. For example, to measure the TRR, officers and 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

An image of a person from the watchlist returned as a result of an alert.

Deployment

The use of an LFR application, 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 deployment, including, but not limited to:

- location
- dates and times

- deployment and watchlist rationale
- legal basis
- necessity
- proportionality
- safeguards
- watchlist composition
- authorising officer
- resources
- relevant statistics
- outcomes
- summary of any issues

Environmental factors

An external element that affects LFR application performance, such as dim lighting, glare, rain or 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

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 to generate possible matches. This is based on digital images (either still or from live camera feeds).

False negative (missed alert)

Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are a number of reasons that false negatives occur, including application, subject and environmental factors, and how high the threshold is set.

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 their questions and helping them to understand of the purpose and nature of the LFR deployment.

LFR operator

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

Person(s) of interest

A person on a watchlist.

Probe image

A facial image that is searched against a watchlist.

Subject factor

A factor linked to the individual, such as:

- demographic factors (for example, sex or ethnicity)
- wearing a heard covering
- smoking
- eating
- looking down at the time of passing the camera

System factor

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

Threshold

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

Watchlist

A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (reference image 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 face recognition.

2. Facial Recognition Overview

LFR in a Law Enforcement Context

2.1 Live Facial Recognition (LFR) is used by Immigration Enforcement (IE) as a precision border security and crime-fighting tactic to identify and locate persons returning in breach of a deportation order (DO), principally for law enforcement purposes.

Live Facial Recognition

2.2 LFR works by analysing key facial features to generate a mathematical representation of them. The representation is then compared against known faces in a Watchlist to identify potential matches against persons of interest.

2.3 Where the system identifies a Possible Match, the LFR system flags an Alert to a trained member of IE personnel who determines if a match is accurate and decides whether to dispatch Engagement Officers, who will undertake further checks and decide upon whether any further action is required. In this way, LFR systems works to assist IE personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

2.4 LFR helps us locate those within a pre-agreed and validated Watchlist by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist which will currently comprise of persons subject to a Deportation Order.

LFR in an Operational Context

2.6 IE will use LFR principally as a law enforcement tool. The proof of concept is focused on identifying those who are seeking to enter the UK in breach of a Deportation Order (DO).

Facial Recognition Products and IE

2.7 IE believes that LFR is a valuable tool that helps IE to keep the public safe and to meet its operational objectives, which includes the prevention and detection of crime, and bringing offenders to justice.

2.8 Whilst appropriate use of LFR as a precision enforcement 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. IE is conscious that the use of LFR has been the subject of much debate. Particular scrutiny relates 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.

2.9 It is therefore the responsibility of IE to ensure that LFR is used lawfully and responsibly for legitimate 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.

2.10 LFR has been used for several years. To address concerns, South Wales Police (SWP) and Metropolitan Police Service (MPS) facilitated academic research by the National Physical Laboratory (NPL) and consulted civil liberty groups. SWP also commissioned NPL to conduct an equitability study on LFR technology in real-world settings, building on previous diligence regarding the FRT algorithm. SWP listened to stakeholders and implemented necessary safeguards. IE acknowledges this work and has adopted similar protocols to ensure best practice and adequate safeguards.

2.11 IE has regard for the national guidance issued to UK police forces and continues to actively engage with the National Police Chiefs Council (NPCC) and the College of Policing.

2.12 For the purposes of the Proof of concept IE are using equipment and staff supplied by South Wales Police (SWP), Home Office and Greater Manchester Police (GMP). SWP and GMP processes and polices relating to the use of LFR are compliant with national Guidance.

2.13 In seeking to address other potential concerns, IE has considered the following legislation, and guidance and commentary:

a. The European Convention on Human Rights (ECHR), in particular Article 8 ECHR

b. Part 3 of the Data Protection Act 2018

c. UK General Data Protection Regulation

d. Immigration Act 1971

e. Borders, Citizenship and Immigration Act 2009

f. Equality Act 2010

g. Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021

h. Information Commissioner's guidance (Law Enforcement | ICO)

i. Borders, immigration and citizenship: privacy information notice

j. Regulating use by law enforcement authorities of live facial recognition technology in public spaces | The Cambridge Law Journal

2.14 IE has carefully considered what safeguards are necessary to support the use of LFR; Watchlists and LFR deployments must be carefully curated and planned and have clearly documented objectives. IE must ensure that their assessment and authorisation clearly articulates legality, necessity, and proportionality.

2.15 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.

- When considering proportionality, IE should consider whether the operation strikes a fair balance between the public benefits from the use of LFR and the infringements with peoples' right to privacy.

- The AO must also be satisfied that LFR Operators and LFR Engagement Officers 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 application Alerts.

- The AO must also consider how the deployment of LFR may impact on communities, that 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.

2.16 IE is not only concerned with developing and implementing precision tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. IE will implement a robust governance process to review the effectiveness and impact of LFR on an ongoing basis. IE 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.

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

3. Strategic Intention, Objectives, and Use Case

3.1 All LFR products and deployments will be conducted in line with IE strategic intentions.

Strategic Intentions

3.2 IE will: -

a. Use overt LFR in a responsible way to locate and identify people who are sought by IE for law enforcement purposes, that currently means those persons who are returning in breach of a Deportation Order.

b. IE will actively target those who attempt to re-enter the UK in breach of a Deportation Order. The use of LFR will provide a capability to more precisely disrupt criminality, reduce harm to the public and increase public safety.

c. Strengthen and develop LFR technology capability to protect the public, reduce serious crime, and to keep the UK safe for everyone.

d. IE will look to share learning and knowledge with other commands with a shared interest in LFR Technology. In particular those falling within the new Border Security Command and Border Force.

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

f. 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.

g. 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 IE LFR SOP (Standard Operating Procedures) and IE LFR Legal Mandate for further details).

h. Transparently identify, manage, and mitigate reputational and organisational risk to IE.

i. Be recognised as a responsible, exemplary, and ethical organisation.

j. IE will ensure LFR is used ethically in order to protect the tactic from reputational harm.

Operational Objectives

3.3 IE will: -

a. adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Operator oversight is active and involved, with the Operator retaining full control and making the decision on whether to act.

b. engage with and provide reassurance to stakeholders and communities, listening and responding to concerns.

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

Technological Objectives

3.4 IE will: -

a. ensure all LFR products are 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 both a enforcement tactic and operational enhancement.

c. look to technology improvements whilst keeping IE model under review.

IE will be using staff and equipment supplied and managed by South Wales Police (SWP) and Greater Manchester Police (GMP) any deployment of their staff will also follow their own guidance and policy.

Use Case

3.5 This document relates to he use of LFR in an overt capacity to identify and locate those within an agreed watchlist, who are persons subject to a Deportation Order. This use case will serve to ensure border integrity and protect the public from harm.

This reflects IE 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. In addition to delivering on strategic goals of enhanced technical capabilities and a more efficient workforce across IE.

3.6 The use of LFR in an overt capacity will be to identify and locate those within an agreed watchlist who are returning in breach of a Deportation Order.

3.7 The proof of concept will be assessed to ensure the validity and potential benefit of each LFR deployment. Additionally, these factors may be utilised to highlight individuals of interest to other government departments public bodies (i.e. Police Forces) to align with other LFR operations.

3.9 IE will keep the use of LFR under review to ensure all LFR products continue to be effective.

3.10 Deployments of LFR will be kept under strict review, with LFR being deployed into areas where it has the greatest potential to assist IE in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why LFR is to be used in accordance with the principles set out in the Legal Mandate and other IE LFR Documents.

3.11 Given that LFR requires a member of IE personnel to review every Alert for a decision as to whether any further action is required, IE will always deploy LFR in a way that is operationally effective and allows IE to act on any Alerts effectively.

3.12 LFR will not be used indiscriminately.

Where can LFR be deployed

3.13 LFR can only be deployed in an area where there is a clear enforcement rationale and intelligence picture. For the proof of concept, it shall only be operated at UK ports. Such deployments must be authorised by the Senior responsible officer for LFR and is also subject to the Authorising officer signing off on the deployment.

4. Overview of LFR Deployment Processes

End-to-End Process

4.1 The end-to-end processes for each deployment of LFR will depend on the intended use and outcome. Individual briefings will be drafted for each of the deployments with full details on effective operation shared with all personnel.

The technical operation of LFR

4.2 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 database of reference images, against which to compare facial images captured from a video or image. 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 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 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 IE will review the Alerts and alert an officer to decide as to whether any further action is required. In this way, the LFR system works to assist personnel to make identifications, rather than acting as an autonomous machine-based process devoid of user input

Key Points

The key points are as follows:

4.3 Live Facial Recognition (LFR)

a. LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are within the agreed Watchlist for that deployment.

b. The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area and as to where the deployment will hold the most benefit.

4.4 General

a. The quality and resolution of images are of vital importance and must be carefully considered.

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

c. 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.

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

Using LFR Deployments Effectively

4.5 Deployments of LFR must be accompanied with robust use cases and be clearly justified in their intentions to comply with legal restrictions on its use.

4.6 There must be sufficient appropriately trained resource to be able to respond to or act against Alerts. This is important to ensure that LFR systems, and the data processed by it, is being effectively used.

4.7 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 and their likely presence are all matters that must be considered when deciding what resources should be available.

4.8 It is also vital that IE is transparent in its use of LFR. As well as using signage, the provision of sufficient resource will allow operators to answer questions that the public may have.

5. Governance, Oversight, and Impact Assessments

Facial Recognition Guidance Stipulations

5.1 Following engagement the following stipulations have been proposed and accepted by Immigration Enforcement:

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

b. It can be evidenced that the technology itself will not result in unacceptable gender or racial accuracy variance into enforcement operations.

c. Each Deployment must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific purpose.

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. Immigration Enforcement 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 Surveillance Camera and Biometric Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

Governance Framework

5.2 Immigration Enforcement LFR Documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:

- Pre-Deployment.
- Operational Deployment.
- Post-Deployment.

Pre-Deployment

5.3 LFR can only be deployed in an area where there is a clear enforcement rationale and intelligence picture. For the proof of concept, it shall only be operated at UK ports. Such deployments must be authorised by the Senior responsible officer for LFR and is also subject to the Authorising officer signing off on the deployment. Authority to deploy LFR is an operational one, where the Authorising Officer (AO) rank is set at an appropriately trained Grade 7.

5.4 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed, and an IE officer of Director grade must be notified in line with the process set out by the operational booklet, LFR application/Written authority document.

5.5 The AO must notify the local police force in the area they are operating and ensure they follow any advice around the use and deployment of LFR in their respective force area. They should also include the relevant Border Force Grade 7 in the event they are operating in or around the port environment.

5.6 Immigration Enforcement documents and records need to be completed in support of each deployment. These are set out as below: -

Document	Explanation
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 (AD/Grade 7 Booklet)	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 and the alternatives that were considered but deemed to be less viable to realise the purpose. The written authority 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 LFR deployment. The written approval must be retained in accordance with relevant legislation or policy and be made available for independent inspection and review as required. The record must be recorded using the operational booklet authority and all documents relating to the deployment must be uploaded on to the digital pocket notebook.
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
Assessments	These include the Community Impact Assessment where necessary, 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 sufficient to address the issues arising from the proposed deployment. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the deployment is not only necessary, but also proportionate. Surveillance Camera Commissioner's Self-Assessment will have been completed by the force providing the LFR technology. It should be available for AO review, if required.

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.

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

Document	**Description**
Immigration Enforcement– Appropriate Policy Documents	Immigration Enforcement policy on the processing of data pursuant to the Data Protecting Act 2018 and UK General Data Protection Regulation relating to LFR
Data Protection Impact Assessment (DPIA)	Immigration Enforcement assessment on the processing of data in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation relating to LFR.
Legal Mandate	Outline of the legal considerations to be addressed in order to use and deploy Live Facial Recognition.
Equality Impact Assessment (EIA)	Outlines the IE considerations of the impacts of LFR in relation to Equality Act 2010.
Standard Operation Procedures (SOPs)	Outlines the operating procedures for LFR deployments.

Operational deployment

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

5.8 The Silver Commander (an officer of at least HMI/SEO grade) must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the deployment.

5.9 The Silver Commander needs to be content: -

- that the use of the LFR remains necessary and proportionate for the purposes identified in the Written Authority Document.

- that the safeguards identified in the written approval remain effective; and that the level of officer support committed to the deployment is enabling Alerts to be responded to effectively.

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

5.10 Deployment may need to be curtailed or postponed due to issues like occlusion (e.g., crowds blocking camera views), bad weather or lighting, or changing operational needs. The Silver Commander has full authority to suspend or end the deployment as necessary.

5.11 The Silver Commander must review and record the deployment at intervals they set, based on the context. Each review should cover legality, necessity, proportionality, LFR performance, and engagement analysis. For the proof of concept pilot this decision will be reviewed on a 2 hourly basis.

Post deployment

5.12 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 tool. A debrief should be conducted after each deployment and a record made of the fact it has been done including any learning points or best practice.

5.13 Each deployment should be subject of an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO to ensure that appropriate senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

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

5.15 Post-Deployment, IE must continue to ensure that the processing of any personal data associated with LFR is conducted in a lawful way and in compliance with IE 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 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.
c. Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 24 hours.

5.16 Where a false alert is generated, IE will look to retain anonymised demographic data in order to investigate any potential bias.

6. Oversight Bodies and Regulatory Framework

6.1 Within IE, the senior internal oversight body for LFR is the Emerging Technology Team within Strategic Services and Transformation.

6.2 IE LFR Legal Mandate sets out the legal framework for IE's use of LFR technology, whilst IE LFR Policy Document supports implementation.

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

a. Biometrics and Surveillance Camera Commissioner (BSCC); The role of the Biometrics and Surveillance Camera Commissioner includes encouraging compliance with the Surveillance Camera Code of Practice, reviewing how the code is working and providing advice to ministers on whether or not the code needs amending. The commissioner is independent of government. See About us - Biometrics and Surveillance Camera Commissioner - GOV.UK (www.gov.uk)

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

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

7. Public Engagement

7.1 Public engagement will be supported using online resources available to the public.

7.2 Some LFR deployments within IE may be negatively affected by publicly advertising its use. Where this is the case IE will take relevant action to ensure its use remains proportionate and, in the public's best interest.

7.3 IE will promote openness with the public and transparency about the use of LFR. Colleagues 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.

7.4 Key stakeholders may be invited to observe the planning and deployment of LFR products.

In Advance of Deployments

7.5 In advance of Live Facial Recognition (LFR) deployments, IE must ensure that:

a. LFR Deployments are, where possible and without undermining the objectives for the Deployment, notified in advance to the public using IE websites – such notifications will give the purpose for the Deployment (for example, to those wanted for Immigration Offences).

b. LFR awareness raising measures (e.g., signs, leaflets and/or website updates) are prepared to support LFR Deployment in line with agreed SOPs.

c. Literature is prepared for persons who may be spoken to (to include information linking to our web page which then links to the Borders, immigration and citizenship: privacy information notice - GOV.UK).

d. External engagement is considered in discussion with IE LFR team. It may be appropriate to pursue engagement opportunities with a number of stakeholders, local authorities, and public consultative or ethical review bodies.

e. 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.

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

7.6 During Live Facial Recognition (LFR) Deployments, IE must ensure that:

a. awareness raising measures are used in line with individual IE LFR SOPs to ensure that the use 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 IE website are available to be handed 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

7.7 After all Deployments, IE must 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 IE website. Care must be taken to ensure that no personal data is published; and

b. external engagement is considered in discussion with IE LFR team. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

.

8. Watchlist Considerations

Compiling Facial Recognition Watchlists

8.1 For the proof of concept, the watchlist will only include those who are subject to an extant Deportation Order. LFR deployments are intelligence-led and reflect current IE priorities and objectives.

Governing Facial Recognition Watchlists

8.2 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.

8.3 IE LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and that inclusion is necessary and proportionate, and that it meets identified enforcement purposes. It helps ensure the public are informed as to the grounds needed to place an image on a Watchlist, and what considerations IE undertake in doing so.

8.4 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 purpose identified, that particular privacy considerations may attach to Immigration 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.

9. Image Quality and LFR Cameras

Image Quality

9.1 The performance of the LFR system is heavily dependent on the quality of the images contained within Home Office databases. The best images are those that are a passport style image that conforms to the Passport Image Guidance.

9.2 Where multiple images of a subject are available; consideration should be given to including the most recent and highest quality image in the Watchlist, to improve the likelihood of locating those who are currently subject to Deportation Order.

Cameras

9.3 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 LFR 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 LFR vendor should advise on specific requirements for their system.

9.4 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.

9.5 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 to maximise the prospects of location.

9.6 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.

9.7 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).

9.8 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 close together, occluding or partly occluding the faces of people (people behind people).

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

9.10 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.

10. Key Performance Metrics

10.1 This section covers the key performance metrics which should be gathered when deploying LFR.

10.2 There are two key metrics that determine the ‘accuracy’ of an LFR system. These are the minimum requirements, and so additional metrics, or indicators may well be relevant and suitable for collation and analysis (these can be specified in individual product SOPs).

True Recognition Rate (TRR)

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

10.4 The TRR is the total number of times an individual(s) on a Watchlist, is known to have passed through the Zone of Recognition or been process by LFR technology and correctly generate an Alert. This is calculated as a proportion of the total number of times individuals passed through the Zone of Recognition or were processed by LFR technology, regardless of whether an Alert is generated by the LFR system or not.

10.5 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)

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

10.7 The FAR is the number of individuals that are either 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 or are processed by LFR systems.

10.8 All of the TRR and FAR metrics should be recorded and reported to the SRO (Senior Responsible Officer). 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 IE, 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.

10.9 Where a false alert is generated, IE will look to retain anonymised demographic data in order to investigate any potential bias.

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

Recognition Time (RT)

10.11 A third important metric, especially with LFR deployments, 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.

10.12 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.

11. Accuracy and Bias

11.1 The Deployment of LFR is informed by IE's Equality Impact Assessment (EIA), which considers the impact of LFR on protected characteristics. Deployments are driven by IE priorities and intelligence-led assessments, both of which determine locality and the purpose. The individuals found on a Watchlist are there because they are currently subject to a Deportation Order.

Addressing Disproportionality

11.2 IE 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. To monitor this, we shall retain anonymised demographic data in the event of a false positive. Moreover, to ensure system functionality, regular tests are carried out using 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.

11.3 South Wales Police (SWP) and Greater Manchester police (GMP) are providing the LFR technology that Immigration Enforcement will be using. SWP carry out scientific bias testing of the LFR system, when necessary, this will be informed by any changes in guidance or updated information provided by the Police LFR systems or supplier and will follow any guidance issued by the College of Policing APP.

11.4 As SWP and GMP will be providing the IE equipment they will manage the technical and assurance aspect of the system for the duration of the pilot. SWP and GMP also have a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. 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, the match reports of the Probe Image and Candidate Images that result in an Alert are retained for the purposes of ensuring accuracy of the system. No Biometric Templates are retained as a result of this. This provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in place for the Deployment, including the reviews undertaken by the Silver and Gold Commanders during the Deployment; and

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

11.5 In August 2021, South Wales Police and Metropolitan Police Service were 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.

11.6 In collaboration with the Metropolitan Police (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. In order to deliver on the objectives of the research, it was necessary to use and document the use of LFR in an operational setting within UK policing. Data collection for the valuation took place in July and August of 2022 alongside five operational deployments of LFR, four in London and one in Cardiff.

11.7 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 so as to appear in the LFR video footage.

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

11.9 The full results are presented in the NPL's report 'Facial Recognition Technology in Law Enforcement Equitability Study'.

11.10 The NPL report gives us an impartial, scientifically underpinned, evidence-based robust analysis of the performance of the LFR FRT System used by SWP in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.

11.13 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 SWP LFR deployments (examples of MPS and SWP figures are given).

11.14 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.

11.15 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)

11.16 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 systems performance is not biased towards any race or gender.**

11.17 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.

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

11.19 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……."

11.20 Having considered the reports finding, and engaged with the police, IE will utilise a threshold of 0.64 for the proof of concept.

11.21 Reflective of the need for continuous improvement, Immigration Enforcement will continue to monitor our use of FRT performance, in terms of both overall system accuracy and demographic differential performance going forward.

12. LFR Policy Summary

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

12.2 It is strongly advised that staff adhere to the document, as this will help ensure that IE 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.

12.3 This document will evolve as technology changes and improves, and as there is further learning from operational deployments.

13. Glossary of Key Terms

Acronym	Title
AD	Assistant Director
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 2000
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
IE	Immigration Enforcement
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LFR	Live Facial Recognition
NPCC	National Police Chiefs' Council
NPL	National Physics Laboratory
ONF	Operational Notification form
RT	Recognition Time
SCC	Surveillance Camera Commissioner

SCCSA	Surveillance Camera Commissioner's Self-Assessment
SOP	Standard Operating Procedure
SWP	South Wales Police
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition