



Immigration
Enforcement

Immigration Enforcement Live Facial Recognition Policy Document

Guidance for Immigration Enforcement (IE) on using overt live facial recognition to locate people of immigration law enforcement interest.

Version No: 2.3
Issue Date: September 2026

Document History

Issue Date	Version No	Produced By	Contents
23/10/2025	1.0	M.WILKINSON	First version
28/01/2026	1.1	J. PARKER	Updated version
16/02/2026	1.1	Internal review	Review updates
18/02/2026	1.1	J. PARKER	Updated version
19/02/2026	2.0	R. GRANGER	Published version
14/04/2026	2.1	M.WILKINSON/J.PARKER	Updated version
15/07/2026	2.2	Internal review	Review updates
19/08/2026	2.3	Review completed	Circulation for SRO sign off
28/09/26	2.3	M.WILKINSON	Signed off by SRO

Final Version Distributed to:

Name	Role
G. Summers	SRO

Table of Contents

Contents

Table of Contents	2
1. Introduction and Policy purpose	5
Aim & Scope	5
Lawful Authority for Overt LFR Deployments	6
Applicable Data Processing Regime	6
2. How the IE Live Facial Recognition (LFR) Policy works from lawful purpose to accountable deployment	7
1. Lawful Purpose is Defined First	7
2. Eligible Individuals are Defined	7
3. Watchlists are Built with Safeguards	8
4. Deployment is Authorised and Planned	8
5. LFR is Used Overtly and with Human Decision Making	8
6. Deployments are Monitored, Reviewed, and Accountable	9
Additional Documents	9
Terminology	10
3. Facial Recognition Overview	15
LFR in an Immigration Enforcement and Criminal Law Enforcement Context	15
Live Facial Recognition	15
Facial Recognition Products and IE	15
4. Strategic Intention, Objectives, and Use Case	18
Strategic Intentions	18
Operational Objectives	19
Technological Objectives	19
Use of LFR	19
Deployments	20
LFR authorisation considerations	20
5. Overview of LFR Deployment Processes	22

End-to-End Process	22
The technical operation of LFR	22
Key Points	23
Live Facial Recognition (LFR)	23
General	23
Using LFR Deployments Effectively	24
6. Governance, Oversight, and Impact Assessments	25
Facial Recognition Guidance Stipulations	25
Governance Framework	25
Pre-Deployment	26
Operational deployment	29
Post deployment	30
Retention	30
8. Public Engagement	33
In Advance of Deployments	33
During Live Facial Recognition (LFR) Deployments	34
After Deployments	34
9. Watchlist Considerations	35
Image Quality	35
Compiling Facial Recognition Watchlists	35
Application and Safeguards	36
Governing Facial Recognition Watchlists	37
Joint deployments	38
Information Governance in Joint Deployments	38
10. Accuracy and Bias	40
Addressing Disproportionality	40
Deployment Specific Equality Considerations	41
11. Design Guidelines for LFR	42
12. Cameras and Camera Placement	43
13. Key Performance Metrics	44

Metrics	44
True Recognition Rate (TRR)	44
False Alert Rate (FAR)	44
Recognition Time (RT)	45
15. Testing Equitability	46
What does this study tell us about accuracy of IE FRT?	46
16. Glossary of Key Terms	49

1. Introduction and Policy purpose

Immigration Enforcement (IE) will run overt Live Facial Recognition (LFR) deployments to support lawful immigration enforcement action, including giving effect to court orders, immigration decisions, and formal criminal justice processes. This may be conducted in partnership with other Migration and Borders and/or law enforcement functions.

This policy document tells IE staff how to use overt LFR to locate relevant people lawfully and ethically, to support IE's and the Home Office's legitimate immigration enforcement aims and summarises the operational use of LFR and the governance and oversight needed to support LFR deployments.

IE staff must follow the agreed LFR policies and processes. This helps IE use LFR lawfully and effectively, with appropriate safeguards, and helps maintain trust and confidence among the public, partners and other stakeholders. More detail about how LFR works and how IE uses it can be found in section 2.

IE recognises the views of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner and continues to acknowledge input from the Science and Technology Ethics Advisory Committee.

IE will review this document regularly and update it as new policy and legislation, guidance and regulations, technology and operational learning develop. Please read this policy alongside the College of Policing APP guidance on live facial recognition.

Aim & Scope

This document aims to:

- Explain to IE staff and the public why IE uses overt LFR, what IE aims to achieve by doing so, and who may be included on a watchlist.
- Set out how IE will compile watchlists and use overt LFR in public places to meet its objectives.
- Explain the governance arrangements for LFR, so that IE uses it lawfully and with appropriate oversight.
- Give an overview of how LFR works and practical steps that help it work well.

IE will publish supporting documents to help members of the public understand how LFR is authorised and used, where it may be used, and the rules and safeguards for adding someone to a watchlist.

Lawful Authority for Overt LFR Deployments

This policy describes how Immigration Enforcement (IE) uses overt Live Facial Recognition (LFR) in public places to support lawful immigration enforcement and criminal law enforcement objectives. Each deployment must identify and record:

- the specific statutory powers and/or legal functions being exercised for the deployment's objective (for example, detention, removal, arrest, or execution of a warrant);
- the applicable data protection processing regime (Part 2 or Part 3 of the Data Protection Act 2018), determined by the primary purposes of the deployment; and
- the safeguards required to ensure any interference with Article 8 rights is lawful, necessary and proportionate.

This policy does not create new powers. LFR is a method of identification used to support the lawful exercise of existing powers and functions. Deployment authority must therefore clearly link the objective (what IE is lawfully doing) to why LFR is necessary for that objective in the specific context.

IE uses LFR overtly. Members of the public are not required to cooperate with having their image captured, and no enforcement action is taken solely on the basis of an LFR alert. Any engagement or enforcement action must be supported by lawful powers and human decision-making, with appropriate verification steps.

Applicable Data Processing Regime

Immigration Enforcement undertakes both administrative immigration functions and criminal law enforcement functions. Where Live Facial Recognition (LFR) is deployed to support administrative immigration activity, including detention or removal under Schedule 2 or Schedule 3 to the Immigration Act 1971, the associated personal data processing is governed by the UK General Data Protection Regulations and Part 2 of the Data Protection Act 2018.

Where LFR is deployed for the prevention, detection, investigation or prosecution of criminal offences, or the execution of criminal penalties, the processing is governed by Part 3 of the Data Protection Act 2018 (law enforcement processing).

This policy applies to both regimes. For each LFR deployment, the applicable processing regime, legal basis, and safeguards must be identified, recorded, and authorised in advance, by reference to the primary purposes of the deployment.

2. How the IE Live Facial Recognition (LFR) Policy works from lawful purpose to accountable deployment

1. Lawful Purpose is Defined First

(Why LFR is used)

Live Facial Recognition may only be used where Immigration Enforcement has a clear, lawful immigration or criminal law enforcement objective, such as:

- Giving effect to deportation orders or court warrants
- Locating individuals lawfully sought for active enforcement or prosecution

LFR is never used for:

- Intelligence gathering
- General monitoring
- Speculative or exploratory purposes

2. Eligible Individuals are Defined

(Who may be on a watchlist)

Only individuals who fall within **strict, objective and predefined categories** may be included on an LFR watchlist, for example:

- Persons subject to an extant Deportation Order
- Persons wanted on a UK court warrant for an immigration related offence
- Persons actively sought for immigration enforcement or removal action, who have failed to comply with immigration conditions of entry or stay or lawful directions, and where their location cannot reasonably be achieved by less intrusive means

Intelligence may inform where and when LFR is deployed. Individuals may be included on a watchlist only if they meet the objectively defined categories in

Section 9; intelligence must not be used in isolation to create eligibility or to expand those categories

3. Watchlists are Built with Safeguards

(How inclusion is controlled)

Watchlists must be:

- **Purpose specific** – linked to a defined deployment objective
- **Time limited** – not reused without fresh authorisation
- **Deployment specific** – tailored to location and context
- **Accurate and minimal** – no broader than necessary

Individuals are included only by reference to the authorised criteria, not by association, speculation, or historic non-compliance alone.

4. Deployment is Authorised and Planned

(When and where LFR may be used)

Before any deployment:

- A necessity and proportionality assessment is completed
- The applicable data protection regime (Part 2 or Part 3 DPA 2018) is identified and complied with
- A Grade 7+ Authorising Officer provides written authority
- DPIA and Equality Impact Assessments are considered
- The deployment location and timing are justified

5. LFR is Used Overtly and with Human Decision Making

(What happens during deployment)

- LFR compares faces only within a defined zone of recognition against the authorised watchlist
- If the system produces an alert, it is reviewed by trained staff
- Humans make all decisions about engagement or enforcement

- No action is taken solely on the basis of a system alert

Images of people who do not generate an alert are automatically and permanently deleted. LFR is a tool that supports Officers in locating relevant persons. It does not replace the Officer's decision-making obligation. Officers must take the final decision about whether to speak to someone or take enforcement action.

6. Deployments are Monitored, Reviewed, and Accountable

(What happens after deployment)

Where appropriate and proportionate, Immigration Enforcement may publish summary information about deployments to support transparency and public trust.

- Outcomes and performance metrics are recorded
- False alerts and system performance are reviewed
- Any issues or learning are documented
- Data is retained or deleted in line with strict time limits. This will be within 24 hours
- Activity is subject to internal oversight and external scrutiny (ICO / BSCC)

Information about deployments is published where appropriate to support transparency and public trust.

Additional Documents

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

- Standard Operating Procedure (SOP)
- Data Protection Impact Assessment (DPIA)
- Equality Impact Assessment (EIA)
- Legal mandate
- Immigration Enforcement Policy documents
- Appropriate Policy Document: processing special category data under UK GDPR and Part 2 DPA 2018
- Appropriate Policy Document on sensitive processing for Law Enforcement Purposes, under Part 3 DPA 2018

Terminology

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

Title	Description
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

Title	Description
	seeding known subjects into a Watchlist and comparing their presence with the number of alerts generated.
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.
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.
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.

Title	Description
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.

Title	Description
Formal decision relating to criminal proceedings	A formal decision means a recorded and auditable decision that has been made to seek an individual's attendance or arrest in connection with criminal proceedings by Immigration Enforcement, Border Force, Criminal Financial Investigators, a UK police force, or UK prosecuting authority. Inclusion on a Watchlist under this category is not based on intelligence interest alone and must be capable of objective justification and review.
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 purposes 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 included on a watchlist solely by reference to the eligibility criteria set out in Section 9.
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 head 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

Title	Description
	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.

3. Facial Recognition Overview

LFR in an Immigration Enforcement and Criminal Law Enforcement Context

Live facial recognition (LFR) is used by Immigration Enforcement (IE) as a targeted immigration and law enforcement tool to help identify and locate people who are wanted by Immigration Enforcement officers, to exercise immigration enforcement powers and enforce court orders or prosecution decisions.

Live Facial Recognition

LFR monitors faces within a defined zone of recognition. LFR works by measuring and comparing key facial features. It turns a face image captured by the cameras deployed into a set of numbers (a biometric template) and compares that template with templates in a watchlist to find possible matches.

If the system finds a possible match, it generates an alert. A trained operator reviews the alert and decides whether it might be a match. Engagement officers carry out further checks and decide whether any action is then required. LFR supports staff decision-making; it does not make decisions by itself.

Facial Recognition Products and IE

IE considers LFR a useful tool to support its immigration enforcement objectives:

- **Stop:** Prevent people from entering the UK illegally, ensure compliance and disrupt the organised crime groups
- **Manage:** Identify those in the UK without status, maintain contact with them and bring their cases to conclusion
- **Remove:** Remove those with no right to be here, especially high-harm individuals
- **Protect:** This underpinning mission recognises the vital role IE plays in protecting the UK public and economy, maintaining the integrity of the immigration system, and safeguarding vulnerable individuals

This also includes the more general objectives of prevention and detection of crime, bringing offenders to justice and enforcing the integrity of the Immigration System.

The following are illustrative examples where LFR may assist Immigration Enforcement with its statutory duties, by identifying and locating:

1. Persons subject to Deportation Orders re-entering the UK via the Common Travel Area.
2. Those subject to a Deportation Order who have returned in breach.
3. Those who are in breach of Immigration laws and who are removable and cannot otherwise be traced by less intrusive means.
4. Those who are wanted on warrant for Immigration related criminal offences.

LFR has been used for several years. South Wales Police (SWP) and Metropolitan Police Service (MPS) have 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 facial recognition technology (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. IE will be using technology that has been subject to academic research led by the National Physics Laboratory (NPL).

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

IE will be using its own equipment and staff for deployments but may on occasion work jointly with other authorised LFR-equipped Police Forces. This may include IE providing watchlists to police to run on their system on behalf of IE or Police providing data to IE to run on IE systems dependant on whose equipment is being used. The authorised LFR-equipped Police Force's processes and policies relating to the use of LFR will be compliant with national guidance.

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

Each deployment must be carefully designed and have clearly documented objectives.

The Authorising Officer (AO) must ensure that their assessment and authorisation is in accordance with applicable data protection law and the IE Live Facial Recognition governance framework.

When considering proportionality under the ECHR, 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.

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 relevant stakeholders.

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

4. Strategic Intention, Objectives, and Use Case

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

Strategic Intentions

IE will:

- Use overt LFR responsibly to help locate and identify people included on an authorised watchlist as they pass through the zone of recognition, for defined immigration enforcement or criminal law enforcement purposes.
- Strengthen and develop LFR technology capability to protect the public, reduce serious crime, and to keep the UK safe for everyone.
- 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.
- Build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns and maximising transparency.
- 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.
- 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).
- Transparently identify, manage, and mitigate organisational risk to IE, ensuring LFR is used ethically and responsibly in order to protect the tactic from reputational harm.
- Be recognised as an exemplary and ethical organisation.

Operational Objectives

IE will:

- Use a **targeted and proportionate** approach when engaging people identified by LFR, with human decision making at every stage. The Engagement Officer remains in control and decides whether to act.
- Engage with stakeholders and communities, listen to concerns, and provide reassurance.
- Identify and review risks linked to LFR, put mitigations in place, and maintain a response plan if those mitigations fail.

Technological Objectives

IE will:

- Make sure LFR products are fit for purpose and deployed effectively, in line with IE's strategic intentions and operational objectives.
- Provide technical oversight and evaluate how well LFR works as an enforcement tool and operational capability.
- Keep the technology and IE operating model under review, and make improvements where needed.

Use of LFR

The use of LFR in an overt capacity will be to identify and locate those within an agreed watchlist.

LFR can help IE use resources more effectively by quickly comparing faces against a pre-defined watchlist. Staff still review alerts and decide what action, if any, to take.

All LFR authorisation requests will be assessed to ensure the validity and potential benefit of each proposed deployment.

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

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 functions. 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.

Deployments

IE will generally use LFR in one of three ways:

- Proactive deployments: planned deployments at locations such as transport hubs and route nexuses.
- Port specific deployments: deployments linked to travel routes and ports.
- Event deployments: deployments linked to a specific event that is expected to increase footfall at a location.

Each deployment category requires a necessity and proportionality assessment that explains why Live Facial Recognition (LFR) is essential and why less invasive methods cannot meet those needs. While intelligence indicates when and where LFR should be used, it does not necessarily identify specific individuals nor replace the specific criteria for adding people to a watchlist.

Information and intelligence may be used to inform the timing and location of Live Facial Recognition deployments (the “where” and “when”). Intelligence may also be used to support verification that an individual already meets an objective watchlist category but must not be used on its own to create eligibility or to add individuals to a watchlist outside the objectively defined categories in Section 9.

LFR authorisation considerations

Deployments must be authorised within the IE LFR governance framework and approved by an LFR Authorising Officer (AO). For higher-risk deployments, Deputy Director (G5)-level oversight must be recorded, either through countersignature on the Written Authority Document or a documented approval route set out in the SOP.

A higher-risk deployment includes one or more of the following:

- high-footfall locations;
- extended deployment duration (beyond the initially approved period);
- deployments outside ports/controlled environments
- locations with heightened community sensitivity;

- complex joint-operational contexts.

For the purposes of this policy, a “controlled environment” means a location where access and movement can be practically managed (for example, through physical layout, managed entry/exit points, queuing systems, or stewarding) so that the zone of recognition and public-facing safeguards can be reliably maintained.

5. Overview of LFR Deployment Processes

End-to-End Process

The end-to-end process for an LFR deployment depends on the purposes and intended outcome. IE will produce a deployment briefing for each deployment and share it with all staff involved.

The technical operation of LFR

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

Stage	Action
1	Compiling or using an existing database of images
	LFR needs a set of reference images (a watchlist) to compare against. The system converts each reference image into a biometric template (numbers that represent facial features).
2	Facial image acquisition
	Cameras capture live images as people move through the zone of recognition. Camera placement helps ensure the system works effectively and supports lawful use.
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.

Stage	Action
5	Face comparison
	The LFR software compares the biometric template with those held on the Watchlist.
6	Matching
	When the system compares two templates, it produces a similarity score. If the score meets or exceeds the authorised threshold, the system generates an alert to indicate a possible match. Trained IE staff review alerts and decide whether any further checks or action are required. LFR supports staff decisions; it does not make decisions by itself.

Key Points

Live Facial Recognition (LFR)

LFR compares faces in the zone of recognition against an authorised watchlist. People are not treated differently unless the system generates an alert and staff assess it to be a valid match.

Camera selection and placement are important to cover the right area and help the deployment achieve its purpose.

General

- The quality and resolution of images are of vital importance and must be carefully considered.
- The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.
- 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.

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

Using LFR Deployments Effectively

Each deployment must have a clear purpose and a documented rationale in accordance with applicable data protection law and the IE Live Facial Recognition governance framework.

IE must have enough trained staff available to review alerts promptly and take any follow-up action.

Deployment planning should consider expected footfall, likely presence of watchlist subjects, and conditions that may affect performance (for example, crowding, lighting and weather). These factors can affect false alerts, missed alerts and response time.

IE must also be open and transparent about LFR use, including clear signage and staff available to answer questions from the public.

6. Governance, Oversight, and Impact Assessments

Facial Recognition Guidance Stipulations

Based on learning from previous deployments and engagement with stakeholders, Immigration Enforcement has adopted the following requirements for LFR.

- Balance the public benefits of LFR with the need to maintain public trust and confidence.
- Use technology that has been tested and monitored so that differences in accuracy across demographic groups are identified and managed, and do not lead to unjustified adverse impacts.
- Assess and authorise each deployment for specific purposes in accordance with applicable data protection law and the IE Live Facial Recognition governance framework
- Train LFR operators to understand key risks (including false alerts and overreliance on system outputs) and hold them accountable for how they respond to alerts.
- Maintain robust governance and oversight that balances the benefits of LFR with its potential intrusiveness. This governance will meet the Home Office Biometric Strategy's transparency requirements, take account of guidance from the Surveillance Camera and Biometrics Commissioner, and reflect feedback from the Information Commissioner's Office and the Science and Technology Ethics Advisory Committee. It will also include a clear internal inspection, audit and compliance regime.

Governance Framework

The Immigration Enforcement LFR documents set out how IE meets these requirements. IE manages governance and oversight in three stages:

- Pre-deployment
- Operational deployment
- Post-deployment

Pre-Deployment

LFR may only be used in locations that have a defined enforcement purpose and are guided by intelligence. Intelligence determines the 'where and when' of deployment; it does not influence the stated criteria for watchlist eligibility.

Deployments must be authorised by the Senior Responsible Officer (SRO) for LFR and approved by an Authorising Officer (AO). Authorisation is an operational decision, and the AO must be an appropriately trained Grade 7 (or higher grade).

Before the AO authorises an LFR deployment in a public place, staff must complete the required documents and notify an Immigration Enforcement Deputy Director (G5), in line with the operational booklet and the written authority process.

The AO must notify the local police force for the area and follow any relevant local advice on LFR. If the deployment is in or near a port, the AO must also include the relevant Border Force Grade 7.

Immigration Enforcement must complete and keep the following documents and records for each deployment:

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

Document	Explanation
	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 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

Document	Explanation
	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, where they are doing so. 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.

IE also maintains the following LFR documents centrally:

Document	Description
Immigration Enforcement – Appropriate Policy Documents	Immigration Enforcement policy on the processing of data pursuant to the Data Protection 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.

Document	Description
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 the Equality Act 2010.
Standard Operation Procedures (SOPs)	Outlines the operating procedures for LFR deployments.

Operational deployment

Staff must record the date, time and location of the deployment accurately.

The Silver Commander (at least HMI/SEO grade) must keep the deployment under review for its duration.

The Silver Commander must be satisfied that:

- LFR remains lawful, necessary and proportionate for the purposes set out in the Written Authority Document.
- The safeguards in the written approval remain effective, and there are enough officers to assess and respond effectively to alerts.
- Conditions (including subject, system and environmental factors) support effective use of LFR for the authorised purposes.

The Silver Commander may need to pause, stop or postpone the deployment if conditions affect performance (for example, crowding that blocks camera views, poor weather, or poor lighting) or if operational needs change. The Silver Commander has authority to suspend or end the deployment where necessary.

The Silver Commander must carry out and record reviews at intervals they set, based on the deployment context.

Post deployment

After each deployment, staff must complete a debrief and record that it took place, including any learning points and good practice. This helps improve future deployments and supports ongoing assessment of whether LFR remains effective and proportionate.

Once LFR is no longer required, the deployment must be cancelled through the authority cancellation process. The LFR Deployment Record must be submitted to the AO to maintain senior oversight. Reports should normally be completed and submitted within 31 days.

IE will evaluate deployment outcomes and use the findings to support oversight and scrutiny.

Retention

The following retention rules apply:

1. Non-alert processing (no alert generated)
 - If the system does not generate an alert, biometric data captured for that person is automatically and permanently deleted as part of the LFR system process.
2. Alerts generated (initial alert stage)
 - Where an alert is generated, IE will retain only the minimum information necessary to support:
 - immediate operational verification;
 - post-deployment accuracy review; and
 - audit and scrutiny requirements.
 - The default retention for alert-related operational data is time-limited and must be specified in the Written Authority Document and Deployment Record by reference to the purposes and applicable processing regime. For operational LFR artefacts (for example, probe/candidate images displayed for operator review and immediate verification), this will be within 24 hours unless the Written Authority Document specifies a shorter period.

3. False alerts

- Where an alert is assessed as a false alert (including confirmed false alerts), IE will delete alert-related personal data within 24 hours, unless a shorter period is specified in the Written Authority Document.
- IE may retain anonymised demographic data and de-identified performance information for the purposes of monitoring accuracy and potential bias. Anonymisation standards and retention periods are set out in the DPIA/SOP.

4. True alerts and outcomes

- Where an alert contributes to an engagement or enforcement outcome, retention and further processing must be governed by the applicable legal framework and operational record-keeping requirements for that outcome (for example, immigration casework records or criminal justice processes).
- LFR data must not be retained longer than necessary for the specific purposes and must be subject to access controls and audit. Where an alert results in an immigration enforcement or criminal justice outcome, any further retention is governed by the applicable casework/criminal justice record-keeping rules; the “within 24 hours” expectation applies only to the LFR system’s operational artefacts for live deployment processing, not to lawful case records created as a result of an encounter.

5. Audit artefacts (match reports)

- For the purpose of post-deployment accuracy and assurance review, IE may retain match reports (for example, probe/candidate image comparison outputs and operator decision logs) for a defined and time-limited period within 24 hours. No biometric matching templates are retained beyond live system processing.

References in this policy to the deletion of alert-related personal data concern operational processing for live deployments. Separate, time-limited retention of audit or assurance material is permitted only to support accuracy review, oversight and accountability, and does not involve the retention of biometric templates.

7. Oversight Bodies and Regulatory Framework

Within IE, the Emerging Technology Team (Strategic Services and Transformation) provides senior internal oversight for LFR.

The IE LFR Legal Mandate explains the legal framework for using LFR. This policy document explains how IE will apply that framework in practice.

IE's use of LFR is also subject to external oversight, including by the Biometrics and Surveillance Camera Commissioner and the Information Commissioner's Office.

8. Public Engagement

IE will support public engagement through information that is available to the public online and during deployments.

Transparency is the default position for Immigration Enforcement's use of LFR. Any departure from advance notice is exceptional, must be justified and recorded, and does not affect the requirement that deployments remain overt and subject to post-deployment publication and scrutiny.

IE will be open and transparent about its use of LFR. Staff should be ready to explain what LFR is, why it is being used, and what safeguards apply. Where appropriate, staff should have information leaflets available to give to members of the public. Leaflets should set out key messages clearly to support public trust and confidence.

IE may continue to invite key stakeholders to observe the planning and delivery of LFR deployments.

In Advance of Deployments

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

- Where possible, and where it will not undermine the deployment's specific objectives, publish advance notice on Home Office websites at least 5 days before the deployment. The notice will explain the purpose of the deployment (for example, to help identify and locate people wanted for immigration offences).
- Prepare awareness materials (for example, signage, leaflets and website updates) in line with the SOPs.
- Prepare written information for people who may be spoken to, including how to find the relevant privacy information notice (via the GOV.UK web page).
- Brief officers on their powers and the limits of those powers. In particular, officers must understand there is no power to require a person to cooperate with having their image captured.
- During any engagement following an alert, remain within their lawful powers and must explain, where appropriate, that cooperation is voluntary unless a separate legal power applies. Refusal to engage does not of itself justify enforcement action. Any further steps must be based on lawful authority and verified identity checks, not the alert alone.

- Consider external engagement (for example, with local authorities and appropriate consultative or ethical bodies). Staff must coordinate this through the IE LFR SPOC before contacting stakeholders.

During Live Facial Recognition (LFR) Deployments

During deployments, IE must ensure that:

- staff use the agreed awareness measures (for example, signage) in line with the SOPs so the public can understand, in general terms, what data is being processed; and
- staff have short notices available to hand out on request, with a brief explanation and information on where to find further details online; and
- officers offer the relevant information to people they engage with, in line with the policy and SOPs.

After Deployments

Immigration Enforcement may publish summary information about deployments to support transparency and public trust about deployments on its website, including:

- Deployment location
- Date of deployment
- Duration of the deployment
- Number of LFR Assets deployed and style of deployment
- Number of Subjects included on a watchlist¹
- The minimum Threshold Setting authorised by the AO
- Number of alerts
- Number of positive alerts (separated into confirmed and unconfirmed)
- Number of false alerts (separated into confirmed and unconfirmed)
- The false alert rate for that Deployment

¹ This is the number of Subjects included across all Watchlists. It is also pertinent to note that an individual may feature on more than one watchlist (for example suspect for offences and wanted on warrant). For the purposes of recording, this would be considered two inclusions in the watchlist.

- Number of outcomes that occurred²
- Number of faces scanned during the deployment³

9. Watchlist Considerations

Image Quality

LFR performance depends heavily on the quality of the images in Home Office databases. The most suitable images are clear, passport-style images that meet current Passport Image Guidance.

IE will follow the standards set by the Surveillance Camera Commissioner in “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”.

[Facing the Camera: Good practice and guidance](#)

If there are multiple images of a subject, IE will use the most recent, highest-quality image to improve the chance of generating an accurate alert.

Compiling Facial Recognition Watchlists

Individuals will **not** be included on an Immigration Enforcement Live Facial Recognition (LFR) watchlist unless they fall within the objectively defined categories set out in this section and there is a current, lawful immigration enforcement or criminal law enforcement purpose for their inclusion.

Individuals will **not** be included on an LFR watchlist solely on the basis of:

- intelligence interest without objective evidence of breaching immigration laws or criminality,
- association with others,
- speculative risk,
- general monitoring,

² This may include arrests, arrangements for voluntary attendance, street bail, and safeguarding actions taken

³ It is important to note that number of faces scanned is not a measure of number of people who have been scanned. This is the number of times the LFR software has identified a face and compared it to the Watchlist. The LFR software does not retain any information (biometric or otherwise) of persons who have been scanned so it is not possible to determine how many times a person may be scanned if they remained in the zone of recognition for a period of time.

For current Live Facial Recognition deployments, Immigration Enforcement watchlists will include only individuals who are lawfully sought for a specific immigration enforcement purpose, where their location or identification cannot reasonably be achieved through less intrusive means, and those who fall within one or more of the following categories.

In respect of those who would principally be sought for criminal law enforcement purposes:

- they are subject to an extant Deportation Order made under immigration legislation, or
- they are wanted on a warrant issued by a court in the United Kingdom in relation to an immigration related offence, or
- they are sought in relation to a charge or charges following a formal decision to seek their attendance or arrest in connection with a criminal immigration related offence⁴,

In respect of those who would be sought for general immigration enforcement purposes:

- they are liable to detention under immigration legislation, or
- they are currently and actively sought for enforcement and/or removal action by Immigration Officers, or
- they have failed to comply with immigration conditions of entry or stay or lawful removal directions.

Application and Safeguards

In all cases:

- Watchlist categories must be pre assessed and authorised as necessary and proportionate for the specific LFR deployment.
- Watchlists must be purpose specific, time-limited, and deployment-specific, and may not be reused for broader or unrelated, or incompatible purposes.

⁴ For the purposes of this category, a **formal decision** means a recorded and auditable decision made by **Immigration Enforcement officers or criminal investigators, a UK police force, or a UK prosecuting authority**, to seek an individual's attendance or arrest in connection with **criminal proceedings**.

- Individuals are included solely by reference to the authorised categories and the defined enforcement purposes, and not on the basis of general interest, intelligence value, or speculative risk.
- Watchlists are subject to documented governance, senior authorisation, and review, ensuring that no broader cohort than necessary is included.
- Individuals will not be included solely on the basis of historic non-compliance where there is no current enforcement purpose
- The necessity and proportionality of each watchlist category must be considered in light of the specific deployment context, including location, duration, and anticipated footfall.
- Individuals under the age of 18 will not be included on IE LFR watchlists.

IE plans LFR deployments using information that has been assessed objectively and reflects current Home Office and IE priorities and objectives.

The IE Legal Mandate explains the legal considerations for compiling a watchlist lawfully. In practice, this means watchlist inclusion must be necessary and proportionate for the defined enforcement purpose.

Key points include keeping the watchlist no larger than needed and taking reasonable steps to confirm that each image correctly identifies the person.

The IE LFR SOP gives practical guidance on how to apply the IE LFR documents when building and using watchlists.

Watchlist size affects how many staff are needed to review and respond to alerts. IE must make sure there are enough trained staff to manage the expected alert volume.

Governing Facial Recognition Watchlists

Systems used to build watchlists are protected by role-based access controls. Staff members who use them must complete role-specific training, including training on data protection.

The IE LFR documents set out how IE will compile, use and manage watchlists lawfully. They require watchlists to be up to date, used only for their defined purpose, and not kept for longer than needed. They also require watchlist inclusion to be necessary and proportionate for the relevant enforcement purpose. Relevant staff should help explain to the public the criteria and safeguards that apply.

Joint deployments

When Immigration Enforcement conducts an operation utilising a partner agency's equipment, Immigration Enforcement remains responsible for securing authorisation for the deployment and any specified watchlist IE wish to run. If another law enforcement agency wishes to provide a watchlist for inclusion, it must be authorised and managed through that agency's own procedures and verifiable authorisation channels. Immigration Enforcement will operate the list on behalf of the other agency; however, any stops or engagements resulting from an alert on that list must be handled by the partner agency and be based on decisions from authorised staff of that partner agency.

When IE collaborates with a partner law enforcement agency's LFR deployment, IE will supply a pre-assessed watchlist for Inclusion into the partner's LFR system. The partner agency will be responsible for authorising the deployment and their own watchlist, while IE will obtain the necessary permissions for the use of their watchlist and assign Immigration staff to respond to any alerts as appropriate. All decisions to engage or undertake action remain with those responding officers.

Information Governance in Joint Deployments

For joint deployments, IE and partner agencies must ensure that information governance roles are clearly documented prior to deployment, including:

- which organisation is the controller for live facial image capture and processing during deployment (typically linked to whose equipment is used and who authorises the deployment);
- which organisation is the controller for watchlist compilation and accuracy of the images supplied;
- the lawful basis and conditions for any sharing of watchlist data or outcomes; and
- how data subject rights requests and complaints will be handled and routed.

Where Immigration Enforcement and a partner agency jointly determine the purposes and means of processing personal data for a joint LFR deployment, the parties will act as joint controllers for the relevant processing. The joint controller arrangement must be documented before deployment, referenced in the Written Authority Document, and reflect the requirements of Article 26 UK GDPR.

The documented arrangement must clearly set out each party's respective responsibilities, including responsibility for authorising the deployment, compiling and assuring any watchlist, operating the LFR system, reviewing alerts, engaging individuals following an alert, recording outcomes, handling data subject rights requests, managing complaints, applying retention and deletion requirements, maintaining audit and assurance records.

10. Accuracy and Bias

This section explains how Immigration Enforcement (IE) works to identify and manage accuracy and bias risks when using live facial recognition (LFR). It summarises the role of Equality Impact Assessments, the steps IE takes to monitor for disproportionate impact, and the safeguards used in deployment planning, watchlist management and system testing.

Each deployment is informed by IE's Equality Impact Assessment (EIA), which considers potential impacts on protected characteristics. Deployment planning is driven by IE priorities and assessed information that supports the deployment's purpose and location.

Addressing Disproportionality

IE recognises the need to reduce the risk of bias and disproportionate impact. Where the system generates a false alert, IE may retain anonymised demographic data so it can monitor performance and investigate potential bias. IE also carries out regular operational checks by using officer and staff volunteers on a "Blue Watchlist". Volunteers walk through the zone of recognition at the start of a deployment to check that the system is working as expected.

LFR technology that Immigration Enforcement will be using was subject to independent testing by the National Physical Laboratory (NPL) in 2023 [[Operational Testing of Facial Recognition Technology](#)]. The National Physical Laboratory report gives an impartial, scientifically underpinned and evidence-based analysis of the performance of the facial recognition algorithm. The report helps us understand the demographic performance of the LFR system and shows that there are settings the algorithm can be operated at where there is no statistical significance between demographic performance. IE are using algorithms which have been considered by the NPL.

Immigration Enforcement, when using their own equipment, has a number of measures in place to guard against a System Factor (system bias) affecting the generation of Alerts. These measures include that:

- those involved in an LFR Deployment monitor all 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

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

Deployment Specific Equality Considerations

For each Live Facial Recognition deployment, the Authorising Officer and Silver Commander must explicitly consider the Equality Impact Assessment and formally note any additional equality considerations for the specific deployment proposed.

The Equality Impact Assessment informs deployment planning and the operational safeguards applied to Live Facial Recognition use. Any additional risks identified must be documented and mitigated prior to deployment authorisation.

11. Design Guidelines for LFR

ISO/IEC 30137-1:2024 (*Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification*) is an international standard on designing and specifying biometric systems used with video surveillance, including facial recognition. IE will use this standard to support the technical design of LFR deployments.

The standard includes guidance on camera selection and placement, threshold settings, watchlist management, and the role of the LFR operator. IE will use it alongside this document and will make sure any technical solution used for LFR is designed and configured to meet these standards.

IE's LFR processes and guidance are designed to support reliable identification using high-definition cameras (2MP and above). For the system to work as intended, the technical components, the operator and the on-the-ground response all need to work together.

A facial recognition system has many components. This section focuses on the components that most affect LFR performance:

1. Cameras (including cabling and network connectivity) and their placement
2. The environment in which the cameras operate
3. The watchlist (reference images and associated metadata)
4. Facial recognition software that detects faces in the video feed, creates biometric templates, compares them against the watchlist, and provides results (for example, an alert or score) to an LFR operator
5. The LFR operator and engagement officers, who review alerts and decide what action (if any) to take
6. Sufficient trained officers to support the deployment and respond to alerts

12. Cameras and Camera Placement

IE must choose cameras that can produce images good enough for facial recognition. Consider image resolution, frame rate, field of view and low-light performance. Current FR systems typically need a facial image with between 20 and 100 pixels between the centres of the subject's eyes (inter eye distance (IED)). The FR vendor can confirm the requirements for the system being used.

Unless you can tightly control the environment, cameras should support wide dynamic range so they can produce good quality images in changing lighting conditions.

Where possible, position cameras to capture faces as close as possible to a 'face on' view (similar to a passport image). This may mean mounting cameras lower than standard CCTV. Consider camera angle and placement in busy areas where faces may be partially blocked by crowds.

Where possible, manage the environment so faces are evenly lit. Avoid strongly directional lighting (for example, strong sunlight). Consider how lighting may change over the day.

The zone of recognition is usually smaller than the camera's full field of view. For example, some faces may be out of focus or may not meet the minimum inter eye distance (IED) needed for facial recognition.

A typical 2MP camera will usually provide enough resolution for LFR to work on a maximum of 3 to 4 people side by side. Consider camera position and the physical environment, including whether you can manage the flow of people through the zone of recognition. If people cluster too closely, faces may be partially blocked (for example, people behind other people).

Detecting and processing faces can place high demand on the system. The LFR software supplier should advise on the hardware required and how many faces can be processed in each video frame. If the system is set to process too many faces, response times may increase. In some cases, the software may skip frames ("dropped frames") to catch up, which can lead to missed alerts.

13. Key Performance Metrics

This section explains the key performance metrics that IE should record for LFR deployments.

Metrics

Two core metrics help IE assess LFR accuracy: true recognition rate (TRR) and false alert rate (FAR). These are the minimum requirements. Other metrics may also be relevant and can be set out in product SOPs.

True Recognition Rate (TRR)

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

TRR is the proportion of times a person on the watchlist passes through the zone of recognition (or is otherwise processed by the system) and the system correctly generates an alert. It is calculated as a proportion of all instances where that watchlist person passes through, whether or not an alert is generated.

You can only calculate TRR if you already know that a watchlist subject has passed through the zone of recognition. One way to do this is to use a “Blue Watchlist” of known volunteers (for example, officers or staff) and record when they walk through the zone. IE and suppliers should not focus only on maximising TRR, because increasing TRR can also increase FAR and create an unmanageable number of false alerts.

False Alert Rate (FAR)

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

FAR is the proportion of people who are not on the watchlist but generate a false alert (including a confirmed false alert), compared with the total number of people who pass through the zone of recognition (or are otherwise processed by the system).

IE should record TRR and FAR and report them to the SRO (Senior Responsible Officer). Operational experience suggests that, in most scenarios, FAR should be 0.1% or less (that is, fewer than 1 in 1,000). The number of false alerts is affected mainly by the number of faces processed and, to a lesser extent, by watchlist size.

Where the system generates a false alert, IE may retain anonymised demographic data to help assess and address any potential bias.

The threshold (the point at which a comparison score triggers an alert) directly affects TRR and FAR. IE must set the threshold carefully to balance finding true matches and keeping false alerts within a manageable level, including the FAR expectations set by the SRO.

Recognition Time (RT)

Recognition time (RT) is the average time between a watchlist subject passing a camera and the system generating an alert. RT does not include the extra time needed for staff to review the alert and decide whether to engage.

RT must be short enough to allow an effective response before the subject moves too far from the point where the alert was generated. Higher-resolution video and more faces per frame require more processing power if RT is to remain low enough to support a real-time response.

15. Testing Equitability

In August 2021, South Wales Police (SWP) and the Metropolitan Police Service (MPS) received Home Office Science, Technology, Analysis & Research (STAR) funding to test the accuracy and equitability of facial recognition technology (FRT) in operational settings. The work covered live facial recognition (LFR), operator initiated facial recognition (OIFR) and retrospective facial recognition (RFR).

The work was delivered by the National Physical Laboratory (NPL) in collaboration with the MPS and was commissioned in late 2021. The NPL is a prestigious world leading centre of excellence that provides cutting-edge measurement science, engineering and technology. To carry out the research, LFR was used and documented during five police deployments in July and August 2022 (four in London and one in Cardiff).

A group of volunteers took part in the study. The group included people of different ages and from different demographic groups. Volunteers walked through the zone of recognition during each deployment so that their faces appeared in the live camera feed.

After the deployments, NPL analysed the data. For the evaluation, NPL used a balanced watchlist (designed to support fair testing across demographic groups) and used facial photographs of the volunteers taken in a range of conditions to reflect operational use for LFR, RFR and OIFR.

The full results are in NPL's report, [Facial Recognition Technology in Law Enforcement Equitability Study](#).

What does this study tell us about accuracy of IE FRT?

The NPL report provides scientifically based impartial evidence on how the SWP LFR system performed in operational conditions, including accuracy and equitability (differences in performance by subject demographics). It also reports on the NEC system used by NPCC LFR police forces.

To summarise LFR performance, NPL reported results for two watchlist sizes: (i) 10,000 reference images (broadly in line with MPS deployments) and (ii) 1,000 reference images (more typical for SWP deployments).

The report uses industry standard measures. These include: (i) True Positive Identification Rate (TPIR), also known as True Recognition Rate (TRR), which measures how often a watchlist subject is correctly recognised when they pass

through the zone of recognition; and (ii) False-Positive Identification Rate (FPIR), also known as False Alert Rate (FAR), which measures how often the system generates a false alert for someone who is not on the watchlist.

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)

For LFR, NPL reported that at a threshold of 0.60, differences in TPIR by gender, race, or race and gender combined were not statistically significant. In other words, the study did not find evidence of a difference in TPIR between these demographic groups at that threshold.

The study also found that at thresholds of 0.60, 0.62 and 0.64, false positives were rare and there was no statistically significant imbalance between demographic groups.

The study reported that, in its data, at a face match threshold of 0.64 or higher there were no false positive identifications. At those thresholds, FPIR was the same across race, age and gender in the study results.

At a threshold of 0.60, NPL reported a statistically significant relationship between TPIR and age, with TPIR improving as subject age increased.

This suggests the system was more likely to recognise watchlist subjects as age increased. NPL also reported that FPIR remained equitable between gender, race and age at this threshold.

NPL noted that performance for under-20s may be influenced by demographic and environmental factors, including subject height and crowding in the zone of recognition:

.....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.....

After considering the report's findings, engaging with UK police facial recognition leads, and deploying LFR with police support, IE will continue to use a threshold of 0.64 for IE-led deployments using approved and objectively tested technology.

IE will continue to monitor FRT performance, including overall accuracy and any differences in performance between demographic groups.

16. Glossary of Key Terms

Acronym	Title
AD	Assistant Director
AO	Authorising Officer (For LFR)
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
FRT	Facial Recognition Technology
FoIA	Freedom of Information Act 2000
GMP	Greater Manchester Police
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

Acronym	Title
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
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition

[OFFICIAL SENSITIVE section starts]

The information in this section has been removed as it is restricted for internal Home Office use.

The information in this section has been removed as it is restricted for internal Home Office use.

[OFFICIAL SENSITIVE section ends]