Home Office

Live Facial Recognition Standard Operating Procedures

October 2025

Document History

22/10/25	1.0	Matt Wilkinson	1st Version

Final Version Distributed to:

Gordon Summers	SRO

Contents

1. Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of enforcement operations.

1.2 All Home office staff must be aware of, and are required to comply with, all relevant HO policy and associated procedures.

1.3 This SOP applies to officers and staff in the following roles: -

a) All operational officers and staff and their supervisors involved in the planning and Deployment of LFR technology; and

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

c) All Authorising Officers (AO); and

d) The operational command team for any LFR Deployment (Gold, Silver and Bronzes); and

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

Note: This list is not intended to be exhaustive.

1.4 LFR Can only be planned and booked through the LFR team.

Terminology

1.5 This SOP focuses exclusively on LFR. Terminology relating to LFR is defined in the IE LFR Policy Document.

2. Authority to Deploy LFR

2.1 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. The authority given by an Authorising Officer (AO) to deploy LFR in support of a policing operation should be made by a Grade 7 (G7) and the Director notified via an operational booklet and LFR Application / Written Authority Document. This should be done 7 days ahead of any deployment. The AO's authorisation should be recorded in writing.

2.2 The LFR Application / Written Authority Document recognises that the intelligence case for the use of LFR may give rise to a single Deployment, or a need for a series of Deployments within a time-limited period. Where the LFR Application / Written Authority Document is to be used to authorise a period of up to 3 days, the form provides for a baseline of safeguards to ensure that the need for the Deployment and the currency in the Watchlist continues to be maintained with due oversight. Should the need to Deploy continue beyond 3 days, a further LFR Application / Written Authority Document must be sought. This approach ensures that the use of LFR is time-limited but allows an operationally effective way to plan for and deliver LFR as part of wider IE strategies.

2.3 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed. Whilst the Director does not provide authority for LFR Deployment, engagement with this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby regional and national issues can be considered as much as possible. This affords the Director the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address any concerns.

2.4 The AO must notify the local police force for the area in which they are operating prior to any deployment. The authorising officer must also complete an

Equalities and Community Impact Assessment (ECIA) in addition to an Operational Notification Form (ONF).

2.5 The authority of the AO: -

a) must articulate the legitimate aim of the Deployment and the legal powers that are being relied upon to support the Deployment; and

b) must confirm that the AO is satisfied that the Deployment complies with IE LFR documents.

c) must, from a Human Rights Act 1998 perspective, articulate (i) how and why the Deployment is necessary (and not just desirable), and (ii) is proportionate (i.e. does the public interest in the LFR deployment strike a fair balance with the infringement to peoples' right to privacy?); and

d) must, from a Data Protection Act 2018 perspective, articulate that it is strictly necessary for law enforcement purposes; meaning the processing is specific and targeted and that there are no less intrusive means of achieving the law enforcement purpose.

e) Necessary on at least one of the following grounds (the ground(s) to be confirmed by AO): -

   i. Necessary for IE's functions[1] and for reasons of substantial public interest; and / or;

   ii. Necessary for the administration of justice.

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

[1] This being defined as "is necessary for the exercise of a function conferred on a person by an enactment or rule of law" in the Data Protection Act 2018. This will typically be the ground relied on to support IE Deployments of LFR since this recognises the powers conferred on an immigration officer by the Immigration Act 1971 and other legislation.

g) confirms the AO is satisfied that the control measures in the Data Protection Impact Assessment and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the Deployment.

h) confirms that the minimum facial matching threshold will be above 0.64 (the level which the NPL report found no bias detected and which is currently used by SWP).

3. ‘Where and when’ - Date, Time, Duration and Location of Deployment

3.1 The AO should define the date, time, location and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate aim, informed by the intelligence case behind the Deployment.

Considerations relevant to a LFR Deployment location

3.2 The intelligence case, enforcement purpose and the environmental factors relevant to a potential Deployment location will substantially inform the potential locations for LFR Deployments.

3.3 Deployment locations will be determined by there being reasonable grounds to suspect that the proposed Deployment location is one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any selected deployment location should be recorded and be capable of being justified.

3.4 The selection of a particular Deployment location may further be supported by:

a) information or intelligence about a proposed Deployment location including if there is an increased public safety risk and/or need to provide public reassurance at a Deployment location; and
b) the ability for officers to take action as a result of an Alert being generated to make Engagements with the public where it is lawful, necessary and proportionate to do so.

3.5 When reviewing a potential Deployment location, AOs must also consider:

- those who are likely to pass the LFR System and the reasonable expectations of privacy the general public may have as a whole at that location.

- some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy Zone 1 central London thoroughfare being typically different to a quiet suburban park or backstreet;

- and the number of cameras used by the LFR System should also be considered in this context to ensure the size and scale of the Deployment enables those on a Watchlist to be effectively located without disproportionately processing biometric data.

3.6 Where there are higher privacy expectations, the AO needs to consider the necessity to Deploy LFR to that location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is necessary (with the processing of data at that site being strictly necessary), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR System against the likely benefits of using LFR. This is to ensure the deployment proposed is not disproportionate to the aim being pursued.

3.7 LFR can only be deployed in an area where there is a clear enforcement rationale and intelligence picture. 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.

Measures during an LFR Deployment

3.8 The public should be notified of LFR Deployments in advance using Home Office website.

3.9 Measures should also be taken during the deployment to ensure the enforcement presence is overt, such that the public can establish that LFR is being used and understand the nature of the data being processed. In addition to the use, uniformed officers and marked LFR camera assets and vehicle,

individuals will be able to see signage placed in advance (outside) of the Zone of Recognition and/or the provision of information leaflets. In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any Deployment is overt, the objectives for the Deployment and its use will also be relevant if the need to Deploy is to be realised. For example, unduly extensive signage may undermine the effectiveness of a Deployment seeking to locate offenders.

3.10 If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of an enforcement power. IE staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.

3.11 Any member of the public who is engaged as part of an LFR Deployment should also be offered an information leaflet about the technology. Any person who requires further information relating to LFR should be provided with contact information for the IE LFR operational team.

4. ‘Who’ - Watchlist Generation and Criteria for an Image’s Inclusion on a Watchlist

4.1 This section covers the composition, generation and management of Watchlists to be used in LFR Deployments and is structured to address;

a) Safeguards relevant to all Watchlists

b) Who may be added to a Watchlist

Safeguards relevant to all Watchlists

4.2 The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria stipulated in this IE LFR SOP and be specific to an operation or to a defined objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:

Requirement	Rationale for the requirement
Intelligence: Watchlists must be driven by an enforcement need and based on the intelligence case The intelligence case must be current and reviewed before each Deployment.	This intelligence-driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR Deployment
Images sources: Home Office Immigration Enforcement must be satisfied that images for use in Watchlists are lawfully held by the Home Office with consideration also being given as to: • the legal basis under which the image has been acquired and retained	This requirement ensures that all images proposed for inclusion are lawfully held by IE – this includes consideration of the legal basis, human rights and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how IE hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance.

Requirement	Rationale for the requirement
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: • is of a person intended for inclusion on a given Watchlist; and; • is the most up to date and/or suitable image available to the Immigration Enforcement that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);	This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that person should they pass the LFR System. This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to IE whilst ensuring those sought are located.
Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment.	This is to ensure only the most recent watchlist is in use and the system is up to date.

Additional safeguards relating to protected characteristics

4.3 IE have completed an Equality Impact Assessment (EIA) for LFR which addresses the protected characteristics under the Equality Act 2010. Prior to any deployment the Authorising officer shall review that document and ensure if any additional mitigation or safeguards are required.

Home Office originated images that may be included on a Watchlist

4.4 Images that may be deemed appropriate for inclusion within an LFR Watchlist are currently limited to Home Office images of persons who are subject to an extant Deportation Order.

4.5 The AO must be satisfied that the individuals included in this Watchlist have been assessed and that the conditions have been lawfully imposed and remain in effect at the time of the Deployment.

5. IE LFR Documents

5.1 Assessments; For each authorised LFR operation, the following assessments need to be created, reviewed, and amended where necessary: -

a) Data Protection Impact Assessment* (Review/Amend/Adopt); and
b) Equality Impact Assessment* (Review/Amend/Adopt); and
c) The Surveillance Camera Commissioner's Self-Assessment (Review/Amend/Adopt) *

Note: *Assessments marked as `Review/Amend/Adopt' have been created by the LFR team and require individual review to ensure their suitability for each LFR operation.

6. LFR Operational Roles

LFR Command Team

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

a) **Gold Commander (minimum G7):** There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their `strategic intention' aligns with the Written Authority Document. Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold can also perform the AO role.

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

c) **Bronze Commander:** Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with sufficient clarity and ensure that they are fully understood by all officers and staff involved in the Deployment.

6.2 Where LFR Deployments form part of a larger overarching operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative

command team terminology or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching operation.

LFR Operator

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

6.4 The LFR Operator must log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR System performance to the Silver Commander.

The LFR Operator's log should include: -

a) the LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; and

b) what decision was taken regarding whether to Engage a member of the public or not; and

c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

LFR Engagement Officer

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

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

6.7 The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place[2]. It must not be an automatic consequence that an Alert results in an Engagement. The LFR Engagement Officer must always be satisfied that there is a match before engaging with an individual. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert. For the proof of concept, the police will operate the LFR equipment. When an alert is generated, the police officer will review the image and if matched, will refer to an Immigration officer who will review. If they agree they will then transmit the description of the person to an Immigration officer who will then approach the passenger and establish identity, nationality and lawful status. The approaching officer will then decide what action if any is then required.

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

6.9 Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

6.10 If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render

[2] The driving force behind this point is that an LFR Operator should not be making the decision that an Engagement Officer carries out an Engagement. LFR Engagement Officer must make their own decision and have a clear understanding of the legal basis supporting any action they take.

them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

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

6.12 Where members of the public choose to avoid an LFR Zone of Recognition, officers are reminded that this alone is insufficient grounds for further inquiry. Immigration officers have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other power where it is right and proper to do so.

LFR System Engineers

6.13 LFR System Engineers have enhanced technical training for the Deployment of LFR (see LFR Policy Document for further information). LFR System Engineers are responsible for the set-up of the LFR equipment and the optimisation of the LFR application to maximise performance. (For the proof-of-concept LFR system engineers will be provided by SWP and GMP as appropriate).

7. Post-Deployment

7.1 Following each LFR Deployment, the Silver Commander must ensure that a post Deployment evaluation is completed which is updated in the Deployment Record. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both qualitative and quantitative in nature.

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

7.3 The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (including what methods were used to obtain them): -

a) total number of individuals and the total number of images included in the Watchlist (there may be multiple images of some individuals); and

b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR application was able to generate a Template from them); and

c) total number of LFR application-generated Alerts; and

d) total number of Alerts that do not result in an Engagement; and

e) total number of Alerts where a decision was taken to Engage an individual; and

f) total number of Alerts that are confirmed as true alert (the individual is who the LFR application suggests they are); and

g) total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and

h) anonymised demographic data relating to any false alerts, in order to investigate any potential bias; and

i) total number of correct Alerts that result in an Engagement that do not require any further action; and

j) outcome of each case where action is instigated following an Alert; and

k) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome; and Threshold setting for the Deployment.

8. Data Retention & Data Management

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

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

8.2 Where the LFR application generates an Alert, all personal data is deleted as soon as practicable and in any case within 24 hours.

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

8.4 IE will not be using CCTV during its deployment.

8.5 The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data must be reported immediately to the AO, Gold, and the Data Protection Officer.

Register of Deployments

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

a) name and rank of the AO and command team; and date, time, duration, and locality of Deployment; and
b) Watchlist composition statistics (not including any personal data); and
c) number of Alerts, broken down as True Alerts and False Alerts including:
    (i) perceived age range

(ii) perceived sex

(iii) perceived race

d) number of Engagements and their results;

8.6 IE will make information relating to LFR Deployments available to the public in accordance with the IE LFR Documents.

9 Contact Information

9.1 The IE LFR team can be contacted using the following email address; IEFacialRecognition@homeoffice.gov.uk

10. Further Documentation

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

a) Information Management APP; Information management | College of Policing

b) National Decision Model; National decision model | College of Policing

c) National Intelligence Management; Intelligence management | College of Policing

d) Home Office Biometric Strategy – Published June 2018; www.gov.uk/government/publications/home-office-biometrics-strategy

e) High Court Ruling – R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin);

   i. High Court Judgment Template

f) Court of Appeal ruling - Bridges v Chief Constable of South Wales [2020] EWCA Civ 1058.

   i. R (Bridges) -v- CC South Wales - Courts and Tribunals Judiciary