Home Office

Live Facial Recognition Standard Operating Procedure

Version 2.0

Contents

Contents 2
About this guidance 3
Contacts 3
Publication 3
Document History 3
Changes from last version of this guidance 4
Introduction 5
Terminology 5
Authority to deploy live facial recognition (LFR) 6
AO approval / operational decision 6
SRO senior ownership / programme-level authority 8
Where and when: Date, time, duration and location of deployment 9
Considerations relevant to an LFR deployment location 9
Measures during an LFR deployment 10
Who: Watchlist generation and criteria for image inclusion 11
Safeguards relevant to all watchlists 11
Additional safeguards relating to protected characteristics 12
Home Office-originated images that may be included on a watchlist 12
IE LFR Documents 14
LFR operational roles 15
LFR command team 15
LFR Operator 15
LFR Engagement Officer 16
LFR system engineers 16
Post-deployment 18
Data retention and data management 20
Register of deployments 20
Contact information 22
Further documentation 23
Pre-deployment assurance checklist 24
Deployment authorisation process flow 30

About this guidance

This guidance tells trained Immigration Officers about deploying with and operating Live Facial Recognition technology in line with required standards and governance.

Contacts

If you have any questions about the guidance and your line manager or senior caseworker cannot help you or you think that the guidance has factual errors then email the IE LFR Team.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance Rules and Forms team.

Publication

Below is information on when this version of the guidance was published:

- version **2.0**
- published for Home Office staff on **5 November 2026**

Document History

Official – sensitive: start of section

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.

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.

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: end of section

Changes from last version of this guidance

Aligned with IE Live Facial Recognition Policy v2.4.

Related content
Contents

Introduction

This Standard Operating Procedure (SOP) sets out the operational procedures to be followed when planning, authorising, deploying, reviewing and closing down Immigration Enforcement use of overt Live Facial Recognition (LFR). It implements the Immigration Enforcement Live Facial Recognition Policy Document, which is the source document for legality, governance, watchlist criteria, transparency, retention and oversight requirements.

All Home Office and Immigration Enforcement staff involved in LFR must comply with the IE LFR Policy Document, this SOP, the applicable Data Protection Impact Assessment, Equality Impact Assessment, Legal Mandate, Written Authority Document and any deployment-specific operational briefing.

This SOP applies to all officers and staff who plan, authorise, support, deploy or act on the results of LFR, including those in the following roles:

- operational officers, staff and supervisors involved in planning and deploying LFR technology;
- officers and staff involved in any investigation or action resulting from an LFR deployment;
- all Authorising Officers (AO);
- the operational command team for any LFR deployment, including gold, silver and bronze roles; and
- LFR Operators, LFR Engagement Officers and LFR system engineers

Note: This list is not exhaustive.

All LFR deployments must be planned and booked through the LFR team.

Terminology

This SOP covers LFR only. The IE LFR Policy Document defines the key LFR terms used in this SOP.

Related content
Contents

Authority to deploy live facial recognition (LFR)

LFR may only be deployed where there is a clear, lawful immigration enforcement or criminal law enforcement objective, a documented enforcement rationale, and a recorded assessment that deployment is lawful, necessary and proportionate. Intelligence and information may inform where and when LFR is deployed but must not create eligibility for inclusion on a watchlist outside the objectively defined policy criteria.

Each deployment must identify the statutory powers or legal functions being exercised and the applicable data protection regime by reference to the primary purpose of the deployment and processing. Where the primary purpose is immigration enforcement, processing must be assessed under UK GDPR and Part 2 of the Data Protection Act 2018. Where the primary purpose is a law enforcement purpose, Part 3 of the Data Protection Act 2018 must be applied. The authorising officer (AO) must record the applicable regime, lawful basis or processing condition, and any relevant safeguards before deployment.

Deployments must be approved by an appropriately trained Grade 7 or above Authorising Officer within the IE LFR governance framework.

AO approval / operational decision

The Authorising Officer (AO) makes the operational decision whether to approve a specific deployment and must be an appropriately trained Grade 7 or above. Before reaching that decision, the AO must personally assess whether the deployment is lawful, necessary and proportionate and whether its operational purpose, legal basis, proposed watchlist, location, timing, safeguards and resources are adequately evidenced.

Before the AO decides the application, the LFR Application, draft Written Authority Document, deployment briefing, relevant DPIA and EIA considerations, operational planning material, watchlist assurance and any information governance arrangements for a joint deployment must be completed and available for review.

The AO must notify the local police force for the deployment area and consider relevant local advice on LFR. Where deployment is in or near a port, the relevant Border Force Grade 7 must also be included in planning and notification. Any higher-risk deployment must obtain and record the required Grade 5 oversight before deployment; this oversight does not replace the AO’s operational decision.

If satisfied, the AO must approve the deployment in writing. The Written Authority Document may authorise a deployment window of up to 30 calendar days for a defined operational purpose, location and set of watchlist criteria, and must state the start and end dates and the conditions and limits of the authority.

The AO’s written authority must:

- state the legitimate aim of the deployment and legal powers relied on to support it
- confirm that the AO is satisfied that the deployment complies with the IE LFR documents
- explain, for Human Rights Act 1998 purposes, why the deployment is necessary and proportionate, including how the public interest has been balanced against the impact on people's right to privacy
- identify whether the processing is governed by UK GDPR and Part 2 of the Data Protection Act 2018, or by Part 3 of the Data Protection Act 2018, by reference to the primary purpose of the deployment
- confirm that processing is necessary on at least 1 lawful ground, as recorded by the AO, including where applicable that processing is necessary for IE's functions and for reasons of substantial public interest, and/or necessary for the administration of justice
- confirm that the AO is satisfied that all reasonable steps have been taken to ensure that the watchlist complies with the IE LFR documents, including legality, necessity and proportionality requirements
- confirm that the AO is satisfied that the control measures in the DPIA and EIA have been reviewed and are appropriate mitigations for the deployment
- state the authority start and end dates, confirm that no more than 10 deployment days may take place during the authorised period, and confirm that deployments may not take place on more than 3 consecutive days
- confirm that the minimum facial matching threshold for IE-led deployments will be set at 0.64

The deployment window is the period during which the authority may be relied upon; it does not authorise continuous deployment. LFR may be deployed on no more than 10 calendar days in total within the window and on no more than 3 consecutive deployment days.

Before each individual deployment commences within the authorised window, an AO must review the prevailing intelligence, operational circumstances, watchlist currency, risks and safeguards. The AO must record confirmation that the deployment remains lawful, necessary and proportionate and is within the scope, conditions and limits of the original authority.

A contemporaneous Deployment Record must be completed and retained for each deployment within the window. It must record the date, location, start and end time, duration, operational purpose, AO review and outcome, cumulative deployment-day count, confirmation that the deployment remained lawful, necessary, proportionate and within scope, and any material issue, amendment, suspension or cancellation.

The AO may amend, suspend or revoke an authority at any time where circumstances change, or the AO is no longer satisfied that deployment remains lawful, necessary or proportionate. A new application and written authority are required where there is a material change to the operational purpose, location, watchlist criteria, risk assessment, safeguards or other relevant circumstances, or where activity is required beyond the authorised period.

The LFR team must ensure that the signed Written Authority Document, supporting assurance records, notifications, pre-deployment reviews and Deployment Records are retained in the agreed location. The deployment must also be reported through the SRO's programme governance and assurance arrangements, with the record clearly distinguishing programme oversight from the AO's operational authorisation decision.

SRO senior ownership / programme-level authority

The SRO for LFR provides senior programme-level ownership and governance assurance that LFR deployment activity operates within the IE LFR governance framework. This relates to overall accountability, governance, risk, policy compliance and strategic oversight. The SRO's programme-assurance role does not replace the AO's operational authorisation decision for a specific deployment. Where the SRO is a Grade 5, the SRO may also provide the G5-level oversight required for a higher-risk deployment, provided the record clearly distinguishes the SRO's programme-assurance role and G5 oversight from the AO's operational authorisation decision.

Related content
Contents

Where and when: Date, time, duration and location of deployment

The AO must define the authorised location, operational purpose and authority period, and ensure that each individual deployment attendance within that period has its own date, start and end time, duration and review record. Each attendance must remain within the maximum 10 deployment days permitted under the authority and the limit of no more than 3 consecutive deployment days. The decision must be based on the legitimate aim, enforcement purpose, intelligence picture and assessment of necessity and proportionality.

Considerations relevant to an LFR deployment location

The intelligence picture, enforcement purpose and environmental factors must inform the choice of deployment location.

A deployment location may be selected only where the AO is satisfied that there is a clear enforcement rationale and intelligence or information supporting the likelihood that 1 or more persons within the authorised watchlist criteria may attend, pass through or be located at that place during the authority period. The reasons for selecting the location must be recorded and capable of justification.

The AO may also take account of both:

- information or intelligence about the proposed deployment location, including any increased public safety risk or need to provide public reassurance
- whether officers can respond effectively to an alert and engage with a person only where it is lawful, necessary and proportionate to do so

When reviewing a potential deployment location, the AO must also consider:

- who is likely to pass through the LFR system and the reasonable privacy expectations people may have at that location
- whether the location has higher privacy expectations than other public places, as described in section 4, “LFR authorisation considerations”, of the IE Live Facial Recognition Policy Document
- whether the number and position of cameras are proportionate to the deployment purpose and do not process more biometric data than necessary

Where privacy expectations are higher, the AO must consider whether LFR is necessary at that location and whether the same aim could be achieved elsewhere. If the location is necessary, the AO must identify practical safeguards and weigh the likely benefits of using LFR against the impact on people whose biometric data may be processed.

Where a location has higher privacy expectations or heightened community sensitivity, the proposed deployment must be treated as higher risk. Deputy Director

(G5)-level oversight must be obtained and recorded before deployment, either through countersignature on the Written Authority Document or through the documented approval route set out in this SOP. This oversight does not replace the AO's operational authorisation decision.

LFR may only be deployed where there is a clear enforcement rationale and intelligence picture. Deployment activity must proceed only within the IE LFR governance framework and must be approved by the AO.

Measures during an LFR deployment

Where possible and where doing so will not undermine the deployment's specific objectives, IE must publish advance notice on Home Office channels at least 5 days before deployment.

Any departure from advance notice must be exceptional, approved by the AO, justified in the Written Authority Document or deployment record, and limited to circumstances where advance publication would undermine the specific authorised objective. The deployment must still remain overt through appropriate measures at the location, including signage, visible deployment assets, uniformed officers or public information materials.

During deployment, IE must use clear measures to show that LFR is being used. These may include uniformed officers, marked LFR camera assets or vehicles, signs placed before the zone of recognition, and information leaflets. The level of public awareness must be enough to make the deployment overt, while still allowing the authorised operational objective to be achieved.

Any member of the public who is engaged as part of an LFR deployment should be offered an information leaflet about the technology. Anyone who asks for more information should be given contact details for the IE LFR operational team.

Related content
Contents

Who: Watchlist generation and criteria for image inclusion

This section explains how watchlists are created, approved, used and managed for LFR deployments. It covers both:

- safeguards that apply to all watchlists
- who may be included on a watchlist

Safeguards relevant to all watchlists

The authorising officer (AO) must approve the criteria for each LFR watchlist. The criteria must meet this SOP, the IE LFR Policy Document and the specific authorised deployment objective. Watchlists and images proposed for inclusion must meet the following requirements:

Requirement	Rationale for the requirement
Operational information and intelligence: Current, assessed information or intelligence may inform the location and timing of a deployment and the overall operational case. It must not, by itself, create eligibility for inclusion or expand the authorised watchlist categories. The information and intelligence supporting the deployment must be reviewed before each deployment.	This supports a targeted and evidence-based deployment while ensuring that the watchlist is compiled using authorised, objective criteria and that its overall scope is necessary and proportionate for the specific deployment.
Image sources: Immigration Enforcement must be satisfied that images proposed for use on watchlists are lawfully held by the Home Office. Consideration must be given to the legal basis on which each image was acquired, retained and may be used.	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. 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.
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image both:	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.

Requirement	Rationale for the requirement
• is of a person intended for inclusion on a given Watchlist • is the most up to date and/or suitable image available to 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 and the prescribed False Alert Rate are 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

IE has completed an Equality Impact Assessment (EIA) for LFR, which addresses the protected characteristics under the Equality Act 2010.

Home Office-originated images that may be included on a watchlist

For current LFR deployments, IE watchlists must only include individuals who are lawfully sought for a specific, current and authorised immigration enforcement or criminal law enforcement purpose, where inclusion is necessary and proportionate for the deployment and the person falls within 1 or more of the objectively defined categories below:

- individuals subject to an extant Deportation Order made under immigration legislation
- individuals wanted on a warrant issued by a court in the United Kingdom in relation to an immigration-related offence

- individuals 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 offence, where their location or identification cannot reasonably be achieved through less intrusive means
- in respect of individuals sought for general immigration enforcement purposes, they must fall within 1 or more of the following categories. In all cases, there must be a current, lawful immigration enforcement purpose for inclusion:
  - they are liable to detention under immigration legislation
  - they are currently and actively sought for enforcement and/or removal action by Immigration Officers
  - they have failed to comply with immigration conditions of entry or stay or lawful removal directions

The AO must be satisfied that the watchlist has been compiled using the authorised criteria and that its overall scope remains necessary and proportionate for the deployment.

Individuals must not be included solely on the basis of intelligence interest, association with others, speculative risk, general monitoring, historic non-compliance where there is no current enforcement purpose, or any purpose outside the authorised policy criteria. Intelligence may inform where and when LFR is deployed and may support verification that an individual already meets an objective category, but it must not create eligibility or expand the authorised categories. Individuals under the age of 18 must not be included on IE LFR watchlists.

Watchlists must be purpose-specific, time-limited, deployment-specific, accurate, minimal and subject to documented governance. They must not be reused for broader, unrelated or incompatible purposes without fresh assessment and authorisation.

Related content
Contents

IE LFR Documents

For each authorised LFR operation, the following assessments must be reviewed and, where necessary, amended:

- Data Protection Impact Assessment
- Equality Impact Assessment
- Surveillance camera self-assessment or equivalent assurance assessment, where applicable

Related content
Contents

LFR operational roles

LFR command team

Each LFR deployment must have a clear command structure. The command structure must include the following roles:

- Gold Commander (minimum G7) - there must be 1 Gold Commander for each LFR deployment. Gold has strategic command and must ensure that the strategic intention aligns with the Written Authority Document - gold remains responsible for ensuring that LFR use stays lawful, necessary and proportionate - gold may also act as the AO
- Silver Commander (HMI / SEO or above) - there must be 1 Silver Commander for each LFR deployment. Silver reports to Gold and has tactical command. Silver may suspend or end the deployment where necessary - silver must keep the deployment under review and ensure that LFR use remains lawful, necessary and proportionate, including whether the safeguards remain effective
- Bronze Commander: Bronze Commanders are responsible for operational activity assigned by Silver and report to Silver. Bronze Commanders should be present at deployment locations unless Silver directs otherwise - if more than 1 Bronze Commander is used, Silver must clearly record each person's responsibilities and ensure that all officers and staff understand the command arrangements

Where an LFR deployment forms part of a wider operation, gold, silver and bronze terminology may be replaced by the wider operation's command structure. The wider command structure may direct the overall operation; however, the review, use and decision-making relating specifically to LFR must remain within the LFR command structure. The command arrangements must be clear, recorded and understood by all officers and staff involved in the LFR deployment.

LFR Operator

LFR Operators must complete the required training before deployment. Their role is to monitor and assess system alerts and, where needed, support LFR Engagement Officers in deciding whether engagement is required.

The LFR Operator must log all alerts to support command reviews during and after deployment. The LFR Operator must tell the Silver Commander about any concerns with system performance.

The LFR Operator's log should include:

- the LFR Operator's assessment of each alert before any decision is made to engage
- the decision on whether to engage with a member of the public
- whether engagement took place and the outcome

LFR Engagement Officer

LFR Engagement Officers must understand the LFR application, how it performs, and how subject, system and environmental factors may affect alerts. They must receive a full operational briefing before deployment and must be deployed in uniform.

When engaging with a member of the public, LFR Engagement Officers must act lawfully, appropriately and proportionately. All staff involved in the deployment and operation of LFR must act in accordance with the Civil Service Code, Home Office Values and this SOP. Wherever possible, anyone engaged following an alert should be offered an LFR information leaflet.

An alert is not an automatic basis for engagement or enforcement action. The LFR Operator and LFR Engagement Officer must assess the alert, taking account of subject, system and environmental factors, before any engagement is considered. Human decision-making must remain central throughout. No action may be taken solely on the basis of an LFR alert. Where engagement is considered appropriate, officers must verify identity and status using lawful checks, remain within their lawful powers, and ensure that any further action is supported by a clear legal basis. Where engagement begins, officers must use appropriate and lawful means to establish the person's identity.

Officers should make enough further enquiries to satisfy themselves that they have grounds to arrest or detain. If officers believe they should use arrest or detention powers before further checks are possible, they must complete any further checks as soon as reasonably practicable. The initial decision must then be reviewed without unnecessary delay.

If a person cannot be identified or does not confirm their identity, that alone is not a criminal offence and does not necessarily justify arrest or enforcement action. Officers must be able to justify any use of powers and must have a lawful basis for any action taken.

Following any engagement prompted by an alert, the LFR Engagement Officer must report whether engagement took place and the outcome to the LFR Operator for recording.

If a member of the public chooses to avoid the zone of recognition, that alone is not enough reason for further enquiry. Immigration officers have no power to direct or compel a person to enter the zone of recognition. This does not prevent officers from engaging with a person where their behaviour or presence gives rise to lawful suspicion or where another lawful power applies.

LFR system engineers

LFR system engineers must have enhanced technical training. They are responsible for setting up the LFR equipment and optimising the LFR application to support

effective performance. For current LFR deployments, system engineers will be provided by the authorised LFR-equipped police force supplying the technology.

Where IE uses LFR technology, technical support or operational support provided by a police force or other partner agency, the deployment documents must record the respective roles, responsibilities and information governance arrangements before deployment. This must include who supplies and manages the watchlist, who has access to deployment data, what information may be shared, retention and deletion responsibilities, and whether a joint-controller arrangement, information-sharing agreement or other governance record is required.

Related content
Contents

Post-deployment

After each live facial recognition (LFR) deployment, the Silver Commander must ensure that a post-deployment evaluation is completed and recorded in the Deployment Record. The evaluation must assess whether the deployment was effective and should include both operational learning and measurable data.

The Deployment Record must also confirm that the attendance took place within the authorised period, remained within the 10-day total and 3-consecutive-day limits, and record any amendment, suspension, cancellation or material issue affecting the authority.

The evaluation must explain which measures were used, how the data was obtained, and what benchmarks were applied. It must also assess whether the safeguards worked effectively, identify any improvements for future deployments, and record how learning will be shared.

The evaluation may include any additional measures that are relevant to the deployment. As a minimum, it must include the metrics in the table below.

Metric	Purpose	Owner / source	Publication status
Total number of people and images included on the watchlist	Checks the scale and proportionality of the watchlist.	Watchlist owner and AO record	May be published in summary form.
Total number of faces processed by the LFR application	Supports calculation of performance and false alert rates.	LFR system log	May be published in summary form.
Total number of alerts generated by the LFR application	Shows how often the system generated possible matches.	LFR Operator log	May be published in summary form.
Alerts not resulting in engagement	Shows how often alerts were assessed and not progressed.	LFR Operator log	Normally internal assurance data.
Alerts resulting in a decision to engage	Shows how often officers decided engagement was justified.	LFR Operator and Engagement Officer logs	May be published in summary form.
Confirmed true alerts	Shows where the person was confirmed to be the person identified by the LFR application.	LFR Operator and Engagement Officer logs	May be published in summary form.
Confirmed false alerts	Shows where the person was confirmed not to be the person	LFR Operator and Engagement Officer logs	May be published in summary form.

Metric	Purpose	Owner / source	Publication status
	identified by the LFR application.		
Anonymised demographic data for false alerts	Supports accuracy, bias monitoring, equality assurance and system review.	Deployment assurance record	May be used only in anonymised or de-identified form.
True alerts requiring no further action	Shows where engagement confirmed identity but no further action was required.	Engagement Officer record	Normally internal assurance data.
Outcomes following alerts	Records action taken following an alert, including any enforcement or no-further-action outcome.	Operational record and casework system where applicable	May be published only in aggregate or summary form.
Engagements not resulting from an alert	Records any non-alert engagement, the reason for it and the outcome.	Operational record	Normally internal assurance data.
Threshold setting used for the deployment	Confirms the authorised matching threshold used and supports performance review.	Written Authority Document and LFR system setting	May be published in summary form.

Demographic information may be recorded only in anonymised or de-identified form for accuracy review, bias monitoring, equality assurance, audit and oversight. It must not be used to make operational decisions about any individual and must not be published in a form that could identify any person. The method of recording must be consistent with the DPIA, EIA and deployment assurance process.

Related content
Contents

Data retention and data management

IE must ensure that all personal data associated with live facial recognition (LFR) is processed lawfully, fairly, securely and only for the authorised deployment purpose. The Written Authority Document and Deployment Record must identify the applicable processing regime, retention requirements, access controls and deletion arrangements for each deployment.

- where the LFR application does not generate an alert, biometric data captured for that person is automatically and permanently deleted as part of the LFR system process
- watchlist import media, temporary operational files and any deployment-specific copies must be securely deleted as soon as practicable and within the authorised retention period recorded for the deployment

Operational alert artefacts created by the LFR system for immediate operator review, including probe images, candidate images or temporary matching outputs, must normally be deleted within 24 hours unless a shorter period is specified in the Written Authority Document. Where an alert leads to a lawful immigration enforcement or criminal justice outcome, any casework or evidential records created as a result of that encounter must be retained only under the applicable casework, criminal justice or records management rules. The 24-hour deletion expectation applies to live deployment operational artefacts, not to lawful records separately created following an encounter.

Where an alert is assessed as a false alert, including a confirmed false alert, alert-related personal data must be deleted 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 accuracy, bias monitoring, oversight and assurance purposes, in accordance with the DPIA and SOP.

No biometric matching templates from live processing may be retained beyond what is necessary for the LFR system to function during deployment. Any audit or assurance material must be time-limited, access-controlled and retained only where necessary for accuracy review, oversight and accountability.

The loss, theft or suspected compromise of any LFR hardware, removable media, deployment record or personal data must be reported immediately to the AO, Gold Commander, Security, the Data Protection Officer and any other required incident reporting route.

Register of deployments

Every LFR deployment must be recorded on a centrally held register. The register must include:

- authority start and end dates, defined location, operational purpose and watchlist criteria
- date, start and end time, duration and locality of each deployment attendance

- the cumulative number of deployment days used under the authority and the consecutive deployment-day count
- the AO's pre-deployment review, outcome and confirmation that the attendance remained lawful, necessary, proportionate and within the original authority
- any amendment, suspension, cancellation or revocation of the authority
- watchlist composition statistics, excluding personal data
- the number of alerts, broken down into true and false alerts, with any demographic information recorded only in anonymised or de-identified form for assurance purposes
- the number of engagements and their outcomes

Demographic information recorded in the register must be used only for accuracy review, bias monitoring, equality assurance, audit and oversight. It must not be used to make operational decisions about any individual, and it must not be published in a form that could identify any person.

IE will make information about LFR deployments available to the public in line with the IE LFR documents.

Related content
Contents

Contact information

The IE LFR team can be contacted at IE Facial Recognition.

Related content
Contents

Further documentation

Further documentation relevant to LFR includes:

- IE LFR Policy Document
- IE LFR Legal Mandate
- Data Protection Impact Assessment
- Equality Impact Assessment
- Written Authority Document
- College of Policing APP guidance and any information governance, joint-controller or information-sharing documentation required for joint deployments

Current external guidance and legal references should be accessed through the approved Home Office or issuing-body source and verified before operational use.

Related content
Contents

Pre-deployment assurance checklist

Official – sensitive: start of section

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

Official – sensitive: end of section

Related content
Contents

Deployment authorisation process flow

Official – sensitive: start of section

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.

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.

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.

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.

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: end of section

Related content
Contents