



Home Office

Immigration Enforcement - Live Facial Recognition Legal Mandate

The legal considerations for IE deployment of overt Live Facial Recognition technology to identify persons of immigration law enforcement interest.

Version No: 2.0

Issue Date: February 2026

Document History

Issue Date	Version No	Produced By	Contents
March 2025	0.1	R Granger	Original outline document
July 2025	0.2	J Parker	Drafting updates
August 2025	0.3	M Wilkinson R Granger	Re-draft and formatting review
September 2025	0.4	M Wilkinson R Granger	Drafting updates and final format review
October 2025	0.5	J Parker	Closing review updates
October 2025	1.0		Final Version
January 2026	1.1	J Parker	Updated version
February 2026	1.1	Internal review	Review updates
February 2026	2.0	R. Granger	Published version

Final Version Distributed to:

Name	Role
G. Summers	SRO

Contents

1. Introduction	3
2. Legal Basis Overview	3
3. Compliance with relevant legislation	5
4. Immigration Act 1971	5
5. Human Rights	5
6. Equality Act 2010	7
7. Protection of Freedoms Act 2012	8
8. LFR watchlist	9
9. Lawful under data protection legislation	9

1.Introduction

This Live Facial Recognition Legal Mandate sets out legal considerations and mitigations taken by Immigration Enforcement ahead of deployments at UK ports.

Live Facial Recognition Technology (LFR) is primarily used by Immigration Enforcement (IE) as a precision tactic to locate people who are attempting to return in breach of an extant Deportation Order (DO), or who are wanted on warrant or are liable for arrest in relation to an immigration-related criminal offence.

Immigration Enforcement (IE) have identified UK ports where intelligence indicates that individuals are either returning in breach of a Deportation Order or are using Common Travel Area routings to avoid formal scrutiny and detection. IE have a key role to play in this area, providing operational support at these ports as and when necessary. The use of Live Facial Recognition (LFR) technology can enhance the Home Office’s intelligence capability by comparing disembarking passengers against a watchlist of individuals subject to extant Deportation Orders or people who are wanted on warrant in relation to an immigration-related criminal offence. LFR should add an additional layer of assurance, particularly in identifying individuals who may have changed their names or used false identities and documents to evade detection, which intelligence indicates has been and remains a current threat to the UK border.

2. Legal Basis Overview

LFR for law enforcement purposes is not subject to dedicated primary legislation but is regulated by several sources of law as well as national and local policies and guidance. The various sources of law combine to provide a multi-layered legal structure to use, regulate and oversee the use of LFR by law enforcement bodies.

Tier one: Legislation	Powers to use LFR	a) Immigration Act 1971, b) The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021 and/or c) Common law power
	Regulating the use of LFR	a) Equality Act 2010 b) Human Rights Act 1998 c) Data Protection Act 2018 (Parts 2 & 3) d) UK General Data Protection Regulation e) Protection of Freedoms Act 2012
	Requests for information in relation to LFR	a) Freedom of Information Act 2000 b) UK General Data Protection Regulation and Data Protection Act 2018 (Subject Access Requests)

Tier two: Code and guidance	Use of LFR	<ul style="list-style-type: none"> a) Secretary of State's Surveillance Camera Code of Practice b) Information Commissioner's Office Code of Practice for Surveillance Cameras and related published ICO opinion - The use of live facial recognition technology by law enforcement in public places- ICO-opinion-the-use-of-LFR-in-public-places.
Tier three: LFR documents	Regulating the use of LFR	<ul style="list-style-type: none"> a) Policy Document b) Equality Impact Assessment c) Standard Operating Procedures d) Operational Guidance and Briefing e) Community Impact Assessment (police) f) Legal mandate g) Signage and Leaflets

Legal basis

To use LFR, IE will rely upon implied powers from the Immigration Act 1971 ("1971 Act"). The UK Supreme Court in *New College London v SSHD* [2013] UKSC 51 confirmed that the 1971 Act provided a range of ancillary and incidental powers to administer the system of immigration control.

Section 24(A1) of the 1971 Act provides that it is a criminal offence for a person to enter the UK in breach of the deportation order. Other relevant immigration-related offences include the facilitation of unlawful immigration under section 25/25A carrying a potential custodial life sentence (sentencing guidelines propose up to 16 years) and knowingly entering without entry clearance which is an offence under section 24(B1) of the 1971 Act with a potential 4-year sentence. Although not exhaustive, these offences are encountered by officers operating within UK ports, involving individuals seeking to avoid detection. Part 3 of the 1971 Act provides for warrants to be sought and obtained in relation to offending under that Part. An implied power from the 1971 Act exists to identify such persons which it is considered the use of LFR falls within. In the alternative, IE would rely upon a common law power to utilise the LFR. In *Bridges v SWP* [2019] EWHC 2341 (Admin), the High Court confirmed that common law powers were sufficient for the police to operate LFR. This finding by the High Court was not disturbed on appeal.

To compile and use the watchlist, IE relies upon an express power in regulation 4 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021.

3. Compliance with relevant legislation

This LFR deployment is being conducted with a partnering police force using a dedicated Immigration Enforcement watchlist that has been specifically prepared and verified for the purposes of the deployment to address criminal offending such as that referenced above.

The Court of Appeal has recognised that the formal legal frameworks which regulate the deployment of LFR, combined with published guidance, can provide sufficient safeguards for the use of LFR to be clear and foreseeable, which is required by Article 8 ECHR: *Bridges v SWP* [2020] EWCA Civ 1058. IE will satisfy this requirement through the publishing of the IE LFR Policy and the Standard Operating Procedures documents so that our deployment of this technology is clear and foreseeable to the public.

4. Immigration Act 1971¹

An Immigration Officer may arrest a person without a warrant under section 28A of the Immigration Act 1971 if the person has committed or attempted to commit a listed offence, or if the Immigration Officer has reasonable grounds for suspecting that the person has committed such an offence. Entering the UK in breach of a deportation order, knowingly entering without entry clearance, and the facilitation of unlawful immigration are such arrestable offences.

This provision therefore allows IE officials to arrest and detain individuals found to have committed or sought to commit such offences, or other offences covered by the 1971 Act.

5. Human Rights

The primary aim for deployments will be for a law enforcement purpose, that is to identify and, where feasible, seek to prosecute individuals returning in breach of a Deportation Order or those who have committed an immigration-related criminal offence.

The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Rights (ECHR)² into domestic British law.

¹ [Immigration Act 1971](#)

² [The European Convention on Human Rights and the Human Rights Act 1998](#)

LFR technology engages the ECHR as it can interfere with an individual's Article 8 ECHR rights - the right to respect for private and family life. It is well-established that the reach of Article 8 ECHR is broad. The case of *S v. United Kingdom* (2009) 48 E.H.R.R 50 confirms that this can relate to a person's biometric data and any storing of data relating to it. The *Bridges* case in the High Court and Court of Appeal considered Article 8 ECHR, specifically in the context of LFR technology, and underlined that operations must be "in accordance with the law" and confirmed that there is an interference with Article 8 ECHR when someone passes through the Zone of Recognition. All IE use of LFR must therefore be proportionate to comply with the ECHR.

In respect of "in accordance with the law" under the ECHR, this can broadly be described as requiring the use of LFR being clear and foreseeable to the public. To satisfy this requirement, IE will publish guidance and SOP which set out who may be placed on a watchlist, where it will operate and relevant safeguards. It will also inform the public of the LFR deployment through appropriate channels, including signage placed before where individuals enter the LFR camera's zone of recognition, and leaflets available both before and within the zone of recognition. Notification of planned deployments will be posted on Immigration Enforcement's dedicated LFR webpage. These notifications will be sufficient to inform the public of the general intent, location and timing of the deployment, without undermining the objectives or operational imperative of that deployment.

In respect of proportionality, LFR interferes with all persons' Article 8 ECHR rights, even those whose images are instantly deleted: *Bridges*. The LFR technology is being deployed in a publicly accessible space where there is existing CCTV, and members of the public would expect to have a reduced level of privacy – accordingly the level of interference is considered to be relatively low. The choice of deployment space is based on IE objectives and quantifiable evidence of a breach of DO encounters and/or those seeking to avoid detection in respect of other immigration-related criminal offences, providing a strong likelihood of people on the watchlist being in the area. The use of the technology is therefore rationally connected to the objective. It is not considered that a less intrusive measure could achieve the objective. Considering all of these matters, the proposed deployment is considered to strike a fair balance between the public interest and the rights of people who will pass through the LFR.

6. Equality Act 2010

The Equality Act 2010³ provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 broadly prohibits discrimination on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, IE must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty (PSED).

IE has completed a detailed EIA to address the PSED which will be published. IE is confident that the use of LFR will not lead to any discrimination/bias.

Immigration Enforcement has adopted a 'human in the loop' approach to ensure that no engagement will occur with a member of the public unless at least one officer has reviewed an LFR system-generated potential match and reached their own opinion that there is a match between the member of the public and the Watchlist image. This means that the LFR system is not making any decision to engage with the public, the officer is making this decision drawing on an image to person comparison, Home Office system records, and their training and experience. Additionally, the officer is best placed to consider the impact of any subject, system and environmental factors which may have influenced the LFR system when it generated an Alert, and if such factors combine to mean an engagement with an individual is not appropriate in the circumstances.

All officers who are part of the LFR trial will have been briefed on the operation of the LFR system, including consideration of factors that can impact performance, and their subsequent conduct, and they will have already received officer training relating to unconscious bias that will support them in undertaking their key role in the Engagement decision-making process relevant to each deployment.

The National Police Chief's Council, national and local Police Force senior officers have been closely consulted and engaged to secure the necessary assurances that the technology selected for use in the pilot has been independently assessed to ensure it does not contain unacceptable bias (e.g. on race and gender grounds). This has been reflected in the Equality Impact Assessment prepared for LFR deployments in accordance with the Equality Act 2010, which demonstrates the objective consideration of the Public Sector Equality Duty. IE will be using staff and equipment supplied and managed by an

³ [Equality Act 2010](#)

authorised LFR-equipped Police Force and any deployment of their staff will also follow their own guidance and policy.

Immigration Enforcement will develop and maintain robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency, whilst taking into account guidance from the Surveillance Camera and Biometric Commissioner and informal consultation feedback from members of the Science and Technology Ethics Advisory Committee. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

7. Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a new surveillance camera code issued by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner.

This includes consideration of the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which IE have had regard. In particular, with respect to LFR, the Code provides:

When using a surveillance camera system for live facial recognition (LFR) purposes to find people on a watchlist, chief police officers should:

- *set out and publish (a) the categories of people to be included on a watchlist and (b) the criteria that will be used in determining when and where to deploy LFR, having regard to the need only to do so for a lawful purpose;*
- *ensure that any biometric data that does not produce an alert against someone on the watchlist by the LFR system is deleted instantaneously or near-instantaneously;*
- *have regard to the Public Sector Equality Duty, in particular taking account of any potential adverse impact that the LFR algorithm may have on members of protected groups;*
- *establish an authorisation process for LFR deployments and identify the criteria by which officers are empowered to issue LFR deployment authorisations*

These points are covered in our policy and Standard Operating Procedures (SOP) which will be published alongside this document.

8. LFR watchlist

The legal power for comprising the watchlist gallery is provided by Part 2 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021⁴. In relation to deployments, these are the legal powers used to take photographs of deportees and other individuals who are subject to warrants in respect of immigration-related criminal offending, and which allow their use for immigration and law enforcement purposes (under Regulation 4).

The Policy document and SOP prepared for the LFR trial set out clear criteria for watchlist inclusion, including the intelligence-based rationale on which it is based and the formal selection, validation and authorisation processes that must be observed in compiling and using the watchlist. To ensure compliance with the SOP, the deployment request must be sent to the Authorising Officer and the Record of Authorisation made by that officer should confirm that the deployment adheres to the principles within it around watchlist generation and compilation, including the criteria that applies to which images may be included on the Watchlist, in what circumstances and for what purpose, to ensure that the necessity and proportionality criteria for the Watchlist are satisfied.

9. Lawful under data protection legislation

The purpose for this processing is covered by section 31 of the Data Protection Act 2018 (DPA 18), which defines “the law enforcement purposes” as “the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. That definition is met by the stated intent of the LFR deployment.

The processing of personal data in the case of LFR is considered sensitive as it is aimed at uniquely identifying an individual using biometric data. The lawful basis for this sensitive processing is section 35(5) DPA 18 – noting that:

⁴ [The Immigration \(Collection, Use and Retention of Biometric Information and Related Amendments\) Regulations 2021](#)

- the processing is strictly necessary for the law enforcement purpose (of preventing, investigating and detecting the criminal offence of persons returning in breach of a Deportation Order or of individuals wanted for arrest in respect of an immigration-related criminal offence);
- a Schedule 8 sensitive processing purpose is met (here being (1)(a) and 1(b) – being necessary for the exercise of a function conferred on IE by an enactment (Immigration Act 1971) and necessary for reasons of substantial public interest (the detection and prosecution of persons returning in breach of a Deportation Order or the wanted for arrest in respect of other immigration-related criminal offending being a substantial public interest); and
- at the time when the processing is carried out an appropriate policy document will be in place.

Section 42 of the DPA 2018 details the requirements of an appropriate policy document. Alongside a Data Protection Impact Assessment (DPIA) that has been reviewed by the Office of the Data Protection Officer, Immigration Enforcement has produced and will publish on GOV.UK a dedicated Policy document, which allows the public to understand details of:

- the data being processed by the LFR system, how often it is processed and whose data is processed;
- procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric data both for those on the Watchlist and those passing an LFR system;
- Immigration Enforcement's policy for the retention and erasure of personal data for LFR processing.

The law enforcement basis for the LFR deployment is also referenced in the [Borders, Immigration and Citizenship: privacy information notice](#) that is published on GOV.UK, which explains how personal information that is legally obtained and held by the Home Office may be lawfully processed in support of the Home Office's statutory functions. In exceptional cases, when the primary purpose (law enforcement) appears not to be appropriate due to individual circumstances, the matched and verified biometric data may then be used for a general immigration purpose, where the data processing is covered by Part 2 of the DPA 2018 and UK General Data Protection Regulation, specifically Article

9(2)(g), which allows for processing of special category personal data (biometric data) where processing is necessary for reasons of substantial public interest. For the reasons stated above, in respect of the Schedule 8 condition, it is considered this threshold would also be satisfied.