Immigration Enforcement

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: 2.3
Issue Date: November 2026

Document History

Issue Date	Version No	Produced By	Contents
March 2025	0.1		Original outline document
July 2025	0.2		Drafting updates
August 2025	0.3		Re-draft and formatting review
September 2025	0.4		Drafting updates and final format review
October 2025	0.5		Closing review updates
October 2025	1.0		Final Version
January 2026	1.1		Updated version
February 2026	1.1	Internal review	Review updates
February 2026	2.0		Published version
July 2026	2.1	Internal review	Review updates
July 2026	2.2		Updates reflecting LFR Policy review
August 2026	2.2	Internal review	Closing review updates
September 2026	2.2		SRO sign off
November 2026	2.3		Updated accountability and oversight wording

Final Version Distributed to:

Name	Role
	SRO

Contents

1. Purpose of this Legal Mandate 3
2. Relationship between this Legal Mandate and the LFR Policy 3
3. What Live Facial Recognition is for IE 3
4. Core legal position 4
5. Statutory immigration functions 4
6. Implied powers under the Immigration Act 1971 5
7. Specific Immigration Act 1971 offences and arrest provisions 5
8. Common law basis recognised in Bridges 6
9. Statutory basis for LFR watchlists 6
10. Watchlists 7
11. Data protection law: identifying the correct regime 7
12. Part 2 DPA 2018 and UK GDPR: administrative immigration processing 8
13. Part 3 Data Protection Act 2018: law enforcement processing 8
14. Sensitive processing under Part 3 DPA 2018 9
15. Appropriate Policy Document under section 42 DPA 2018 9
16. Home Office privacy information and transparency 10
17. Human Rights Act 1998 and Article 8 ECHR 10
18. Necessity and proportionality 11
19. Foreseeability and public information 12
20. Equality Act 2010 and Public Sector Equality Duty 13
21. Protection of Freedoms Act 2012 and surveillance camera principles 13
22. Human decision-making 14
23. Retention and deletion 14
24. Joint deployments and controller responsibilities 15
25. Accountability and oversight 15

1. Purpose of this Legal Mandate

This Legal Mandate explains the legal basis on which Immigration Enforcement uses overt Live Facial Recognition technology.

It details:

- the statutory powers and functions that support the use of Live Facial Recognition;
- the specific legal bases for using biometric information;
- how Immigration Enforcement (IE) complies with human rights, data protection and equality law;
- the safeguards that must apply before, during and after deployments; and
- how the public is informed about the use of Live Facial Recognition.

This document offers a legally grounded explanation about Immigration Enforcement's use of LFR. It does not replace the Immigration Enforcement Live Facial Recognition Policy, Standard Operating Procedures, Data Protection Impact Assessment, Equality Impact Assessment or operational authorisation documents. Those documents explain how Live Facial Recognition is governed and operated in practice.

2. Relationship between this Legal Mandate and the LFR Policy

The Immigration Enforcement Live Facial Recognition Policy explains how Immigration Enforcement uses Live Facial Recognition in practice. The Policy gives operational effect to the legal principles contained within this Mandate and must be read consistently with them. Where operational processes are described in the Policy, those processes are intended to ensure continued compliance with the legal requirements explained in this document.

The Legal Mandate and the Policy therefore operate together as complementary documents:

- the Legal Mandate explains the legal basis for the use of Live Facial Recognition;
- the Policy explains operational controls, governance arrangements and procedures through which Immigration Enforcement applies that legal basis in practice.

3. What Live Facial Recognition is for IE

Live Facial Recognition is a biometric identification tool. It compares facial images captured by cameras during an authorised deployment against a pre-approved watchlist of

people who are lawfully sought by Immigration Enforcement or, where relevant, another authorised law enforcement body.

If the system identifies a possible match, it generates an alert. That alert must be reviewed by trained staff. The system does not decide whether a person is stopped, spoken to, arrested, detained, removed or otherwise subject to enforcement action. Any such decision must be made by officers using their legal powers and professional judgement.

Live Facial Recognition does not create any new enforcement powers. It is a method of identification used to support the lawful exercise of powers that already exist in law.

4. Core legal position

Immigration Enforcement uses Live Facial Recognition only where there is a clear lawful purpose connected to immigration control, immigration enforcement, border security, removal, deportation or immigration-related criminal offending.

The legal framework for this use is multi-layered. It includes:

- statutory immigration powers;
- ancillary and incidental powers needed to administer immigration control;
- express powers to collect, retain and use biometric information;
- aviation and maritime security legislation;
- data protection law;
- human rights law;
- equality law;
- surveillance camera legislation and guidance;
- published Home Office privacy information; and
- deployment-specific safeguards and authorisation requirements.

5. Statutory immigration functions

Immigration Enforcement exercises statutory functions under a range of immigration legislation. These include:

- Immigration Act 1971;
- Immigration and Asylum Act 1999;
- UK Borders Act 2007;

- Borders, Citizenship and Immigration Act 2009;
- Immigration Act 2014;
- Immigration Act 2016; and
- Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021.

These laws support functions relating to immigration control, examination, identity management, detention, removal, deportation, investigation of immigration offending and the enforcement of immigration law.

Immigration Enforcement will rely on these statutory functions when using Live Facial Recognition as a capability to help identify and locate individuals who are lawfully sought for administrative immigration enforcement or immigration-related criminal law enforcement purposes.

6. Implied powers under the Immigration Act 1971

The Immigration Act 1971 is a central part of the legal framework for immigration control.

In *New London College Ltd v Secretary of State for the Home Department* [2013] UKSC 51 (Supreme Court), the Supreme Court confirmed that the statutory powers in the Immigration Act 1971 extended to a range of ancillary and incidental powers needed to administer the immigration control.

Immigration Enforcement relies on those powers where Live Facial Recognition is used as an identification tool to support and inform the lawful administration and enforcement of immigration control.

This means that Live Facial Recognition is not used as a free-standing power. It is used to help Immigration Enforcement identify people in circumstances where identification is necessary to carry out existing statutory immigration functions.

7. Specific Immigration Act 1971 offences and arrest provisions

Live Facial Recognition may support Immigration Enforcement in locating people who are lawfully sought in connection with immigration-related offending.

Relevant offences under the Immigration Act 1971 include:

- entering the United Kingdom in breach of a deportation order under section 24(A1);
- entering the United Kingdom without required entry clearance leave to enter under section 24(B1);

- overstaying their immigration permission under section 24(C1);
- arriving in the UK without the required entry clearance under section 24(D1);
- facilitation of unlawful immigration to the UK under sections 25 and 25A; and
- other offences under Part 3 of the Immigration Act 1971.

Part 3 of the Immigration Act 1971 also provides for warrants to be sought and obtained in relation to offences under that Part.

Section 28A of the Immigration Act 1971 allows an Immigration Officer to arrest a person without a warrant where the person has committed, attempted to commit, or is reasonably suspected of having committed, a listed immigration offence.

Live Facial Recognition may assist officers in identifying a person who is lawfully sought. Any arrest, detention or other action must be justified by the relevant statutory power.

8. Common law basis recognised in Bridges

Immigration Enforcement's primary basis for using Live Facial Recognition rests on statutory immigration functions and implied and ancillary powers.

The courts have also recognised that common law powers can support the use of Live Facial Recognition by law enforcement bodies. In *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), the High Court accepted that common law powers were sufficient for police use of Live Facial Recognition. That finding was not disturbed by the Court of Appeal.

Immigration Enforcement's position is that Live Facial Recognition is supported by its statutory immigration functions and implied and ancillary powers, both administrative and criminal. The common law position recognised in *Bridges* further supports the lawfulness of using Live Facial Recognition as a tested identification tool where it is properly authorised, necessary, proportionate and subject to safeguards.

9. Statutory basis for LFR watchlists

Live Facial Recognition involves the processing of biometric information, against images contained on a watchlist.

Immigration Enforcement relies on Regulation 4 of the Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021 for compiling and using watchlists utilised in Live Facial Recognition.

Immigration Enforcement will only use biometric information for Live Facial Recognition where that use is linked to a lawful immigration or law enforcement purpose and is necessary and proportionate for the deployment.

10. Watchlists

Live Facial Recognition compares faces against a watchlist. A watchlist is a deployment-specific list of authorised reference images and associated identifiers.

Individuals must only be included on a watchlist where:

- they fall within an authorised and objectively defined category;
- there is a current lawful immigration or law enforcement purpose for their inclusion;
- inclusion is necessary and proportionate;
- the image and associated information are accurate and current; and
- less intrusive means are not sufficient in the circumstances.

Watchlists must be:

- purpose-specific;
- deployment-specific;
- time-limited;
- no broader than necessary;
- subject to authorisation; and
- reviewed and deleted in accordance with retention requirements.

Information or intelligence may inform where and when Live Facial Recognition is deployed. It may also help verify whether a person already meets an authorised watchlist category. Information or intelligence alone must not be used to create eligibility for watchlist inclusion or to expand the approved inclusion categories.

11. Data protection law: identifying the correct regime

Immigration Enforcement undertakes both administrative immigration functions and criminal law enforcement functions. The data protection regime that applies to a Live Facial Recognition deployment is determined by the primary purpose of the deployment.

Where the primary purpose is administrative immigration activity, including for addressing non-compliant behaviour and for enforced returns, processing is governed by:

- UK GDPR; and
- Part 2 of the Data Protection Act 2018.

Where the primary purpose is the prevention, detection, investigation or prosecution of criminal offences, or the execution of criminal penalties, processing is governed by:

- Part 3 of the Data Protection Act 2018.

For each deployment, Immigration Enforcement must identify and record:

- the lawful purpose;
- the statutory powers or functions being exercised;
- the applicable data protection regime;
- the lawful basis for processing;
- the biometric or sensitive processing condition relied upon; and
- the safeguards that apply.

12. Part 2 DPA 2018 and UK GDPR: administrative immigration processing

Where the primary purpose of a deployment is administrative immigration enforcement, processing is governed by UK GDPR and Part 2 of the Data Protection Act 2018.

For personal data, Immigration Enforcement relies on Article 6(1)(e) UK GDPR. This applies where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For special category data, including biometric data used to uniquely identify an individual, Immigration Enforcement relies on Article 9(2)(g) UK GDPR. This applies where processing is necessary for reasons of substantial public interest.

The relevant substantial public interest is linked to Immigration Enforcement's statutory functions, including immigration control, enforcement, removal, deportation, identity management and the protection of the borders and immigration system.

Where criminal offence data is processed incidentally within a Part 2 deployment, Immigration Enforcement must ensure that Article 10 UK GDPR and any relevant Schedule 1 Data Protection Act 2018 conditions are satisfied.

13. Part 3 Data Protection Act 2018: law enforcement processing

Where Live Facial Recognition is used for law enforcement purposes, Immigration Enforcement processes personal data under Part 3 of the Data Protection Act 2018.

Section 31 of the Data Protection Act 2018 defines “law enforcement purposes” as the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including safeguarding against and preventing threats to public security.

Immigration Enforcement relies on this basis where Live Facial Recognition is used to support law enforcement activity, including identifying and locating individuals lawfully sought in connection with immigration-related criminal offending, deportation order breaches, warrants or other criminal law enforcement activity.

14. Sensitive processing under Part 3 DPA 2018

Live Facial Recognition involves biometric data processed for the purpose of uniquely identifying an individual. This is sensitive processing under Part 3 of the Data Protection Act 2018.

Where Part 3 applies, Immigration Enforcement relies on section 35(5) of the Data Protection Act 2018. This requires the processing to be strictly necessary for the law enforcement purpose.

Immigration Enforcement will meet that requirement where the use of Live Facial Recognition is strictly necessary to identify and locate persons lawfully sought for a specific law enforcement purpose, and where the same objective cannot be achieved by less intrusive means.

Immigration Enforcement also relies on Schedule 8 to the Data Protection Act 2018. In particular:

- paragraph 1(a), where processing is necessary for the exercise of a function conferred on Immigration Enforcement by an enactment; and

- paragraph 1(b), where processing is necessary for reasons of substantial public interest.

The substantial public interest includes prevention, detection and investigation of immigration-related criminal offending, the enforcement of deportation decisions, the apprehension of offenders, and the protection of the public and the integrity of the immigration system.

15. Appropriate Policy Document under section 42 DPA 2018

Section 42 of the Data Protection Act 2018 requires an Appropriate Policy Document to be in place when sensitive processing is carried out under relevant Schedule 8 conditions.

Immigration Enforcement has and will maintain an Appropriate Policy Document and an associated policy framework for the use of Live Facial Recognition. This shall explain:

- what information is processed;

- whose information is processed;
- why the information is processed;
- the safeguards that apply;
- how data protection principles are met;
- how information is retained and deleted; and
- how accountability is maintained.

The Live Facial Recognition Policy, Data Protection Impact Assessment and related governance documents support this requirement and provide further information about safeguards and accountability.

16. Home Office privacy information and transparency

The Home Office publishes the Borders, immigration and citizenship: privacy information notice. This notice explains how personal information may be used for border, immigration, citizenship and related law enforcement functions.

The notice explains that the Home Office holds and processes personal information for purposes including entering or leaving the UK, securing the border, enforcing immigration laws, law enforcement for criminal matters and other lawful matters.

It also explains that the Home Office processes personal information to fulfil its legal and official functions and will use personal information only where the law allows and where it is necessary and proportionate.

Live Facial Recognition operates within this wider published Home Office transparency framework. It is one method by which Immigration Enforcement processes information to support existing statutory functions.

17. Human Rights Act 1998 and Article 8 ECHR

The Human Rights Act 1998 incorporates Convention rights into domestic law.

Article 8 of the European Convention on Human Rights protects the right to respect for private and family life. Live Facial Recognition engages Article 8 because biometric processing can interfere with a person's privacy rights.

The *Bridges* case confirmed that Article 8 is engaged when a person passes through the zone of recognition during a Live Facial Recognition deployment. It also confirmed that the use of Live Facial Recognition must be in accordance with the law and supported by sufficient safeguards.

Immigration Enforcement will therefore use Live Facial Recognition only where the deployment is:

- lawful;
- necessary;
- proportionate;
- clear and foreseeable;
- subject to objective limits; and
- supported by appropriate safeguards.

18. Necessity and proportionality

For each deployment, Immigration Enforcement must assess whether Live Facial Recognition is necessary and proportionate.

Immigration Enforcement uses Live Facial Recognition because it provides a targeted method of identifying individuals who are lawfully sought and whose identity, whereabouts or presence cannot reasonably be established through less intrusive means alone.

Live Facial Recognition is not deployed simply because the technology is available. It is deployed because it is assessed as necessary to support a specific immigration enforcement or criminal law enforcement objective in circumstances where alternative methods would be less effective, less efficient or less capable of achieving that objective. This assessment must be documented as part of the deployment authorisation process.

That assessment must consider:

- the lawful objective of the deployment;
- why identification is necessary;
- why Live Facial Recognition is necessary to achieve that objective;
- whether less intrusive means would be effective;
- the expected benefit to immigration enforcement or law enforcement;
- the impact on people passing through the zone of recognition;
- the watchlist size and categories;
- the location, timing and duration of the deployment;
- the safeguards in place; and
- the arrangements for retention, deletion, audit and oversight.

Live Facial Recognition must not be used where the same objective can reasonably be achieved by less intrusive means.

19. Foreseeability and public information

For Live Facial Recognition to be "in accordance with the law" under Article 8, the legal framework governing its use must be sufficiently accessible, clear and foreseeable. The courts have confirmed that individuals must be able to understand, in broad terms, the circumstances in which Live Facial Recognition may be used and the safeguards that govern its use.

Immigration Enforcement satisfies this requirement through the publication of documents and relevant information that explain how Live Facial Recognition is governed and used.

These include:

- this Legal Mandate;
- the Immigration Enforcement Live Facial Recognition Policy;
- the Borders, Immigration and Citizenship Privacy Information Notice;
- Data Protection Impact Assessment;
- Equality Impact Assessment;
- public deployment notices;
- signage and public information materials;
- Standard Operating Procedures; and
- supporting governance documentation where appropriate.

Together these documents explain:

- why Live Facial Recognition is used;
- who may be included on a watchlist;
- the legal framework governing its use;
- the safeguards that apply;
- how personal data is processed;
- how information is retained and deleted;
- how rights may be exercised; and

- how concerns or complaints may be raised.

Immigration Enforcement will continue to publish information sufficient to ensure that the use of Live Facial Recognition remains transparent, legally foreseeable and subject to public scrutiny.

20. Equality Act 2010 and Public Sector Equality Duty

Immigration Enforcement must comply with the Equality Act 2010.

Section 149 of the Equality Act 2010 sets out the Public Sector Equality Duty. Immigration Enforcement must have due regard to the need to:

- eliminate unlawful discrimination;
- advance equality of opportunity; and
- foster good relations between people who share protected characteristics and those who do not.

Immigration Enforcement has and will maintain an Equality Impact Assessment for Live Facial Recognition. This assessment will consider potential impacts on protected groups and the safeguards needed to reduce the risk of unfair or discriminatory outcomes.

All alerts must be subject to human review. The system does not decide whether a person is engaged. Trained officers must assess any alert before further action is taken.

21. Protection of Freedoms Act 2012 and surveillance camera principles

The Protection of Freedoms Act 2012 provides for the Surveillance Camera Code of Practice.

The Code includes principles relevant to overt surveillance camera systems and automated recognition technologies. These principles include:

- publishing the categories of people who may be included on a watchlist;
- publishing criteria for when and where Live Facial Recognition may be deployed;
- deleting biometric data that does not produce an alert instantaneously or near-instantaneously;
- having regard to the Public Sector Equality Duty; and
- establishing an authorisation process for deployments.

Immigration Enforcement will apply these principles through its Live Facial Recognition Policy, Standard Operating Procedures, authorisation process, public information and retention controls.

22. Human decision-making

Live Facial Recognition supports human decision-making. It does not replace it.

Immigration Enforcement operates a human-in-the-loop model. This means:

- system alerts must be reviewed by trained staff;
- officers must consider whether the alert appears to be a true match;
- further verification must take place where appropriate;
- officers must consider subject, system and environmental factors;
- no enforcement action must be taken solely on the basis of an alert; and
- any action must be supported by an existing legal power.

23. Retention and deletion

Immigration Enforcement must retain personal data only for as long as necessary.

Where a person passes through the zone of recognition and does not generate an alert, biometric data relating to that person is automatically, immediately and permanently deleted as part of the Live Facial Recognition process.

Where an alert is generated, Immigration Enforcement will retain only the minimum information necessary for lawful purposes such as:

- immediate operational verification;
- enforcement action;
- audit;
- oversight;
- accuracy review;
- complaint handling;
- legal proceedings; or
- lawful operational record keeping.

False alert data must and will be subject to strict deletion controls. Any continued retention must have a lawful basis, be documented and be no longer than necessary.

24. Joint deployments and controller responsibilities

Immigration Enforcement may work with policing partners or other authorised bodies in relation to Live Facial Recognition deployments.

The precise allocation of responsibilities during a deployment depends upon the operational model being used.

Immigration Enforcement may act as:

- a controller;
- a joint controller;
- a processor acting on behalf of another organisation.

The applicable role will be identified and documented before processing begins and will determine the legal obligations that apply to each organisation involved in the deployment.

Specific responsibilities and governance arrangements for Joint Deployments are detailed in the current Immigration Enforcement Live Facial Recognition Policy Document.

25. Accountability and oversight

Immigration Enforcement's use of Live Facial Recognition must be supported by:

- this Legal Mandate;
- a published Live Facial Recognition Policy;
- Standard Operating Procedures;
- Data Protection Impact Assessments;
- Equality Impact Assessments;
- authorisation records;
- watchlist approval records;
- audit and deletion records;
- governance review;
- staff training; and

- post-deployment evaluation.

In developing its approach to Live Facial Recognition, IE has had regard to relevant regulatory, ethical and surveillance guidance, including published guidance, alongside relevant ethical advice.