

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

1.0 Summary of Change

3.24.8 – recent Cambridge and NPL results.

3.25.3 – additional comment about the recent testing and threshold setting.

2.0 What this Policy is About

2.1 This policy relates to the use and governance of Live Facial Recognition technology. This is software procured by Essex Police for operational deployment across the Force. In particular, the parameters and legal constraints will be outlined to ensure that applications of use are in line with the APP and recent legislation.

2.2 This policy will reference appropriate associated procedure documents regarding LFR, links to the college APP and national guidance. More detail about how EP will use LFR can be found in section 6 and within the linked procedure.

2.3 EP is also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics and Surveillance Camera Commissioner, the recent academic based testing of our LFR system, and has participated in the development of national guidance and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).

2.4 This policy seeks to provide EP personnel and members of the public with information about EP's present strategic, operational and technology objectives for the overt use of LFR, such that it enables EP to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives).

2.5 There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR), which relates to non-real time searching of images against a database. Also, not in scope is Operator Initiated Facial Recognition (OIFR) where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis and most importantly not in a 'live' function.

Compliance with this policy and any linked procedures is mandatory.

3.0 Statement of Policy

3.1 Live Facial Recognition (LFR) assists Essex Police (EP) as a precision crime-fighting tactic to locate people who are wanted for criminal offences, reduce violence and protect the most vulnerable in society. This policy and associated procedure documentation will provide instruction for police officers and staff regarding the appropriate legal and legitimate use of LFR.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.1.1 LFR technology uses a live camera feed to scan facial images of a crowd and users advanced algorithms to instantly check against a pre-determined watchlist. If the facial image is not on the watchlist then the image is disregarded immediately.

3.1.2 The aim of the policy is to provide EP personnel and members of the public with the necessary information about the Force's – strategic, operational, and overall objectives for the overt use of LFR. All of which will be done in an ethical manner in line with data protection legislation.

3.1.3 The policy will set out the governance structure in terms of applications, authorities, and then operational deployments.

3.1.4 Its important to note that this policy will not detail or provide guidance / governance on other facial recognition technology such as Retrospective Facial Recognition (RFR) which relates to using FR technology to compare an unknown image of a suspect against a database to assist with identification of that person. The policy also doesn't include Operator Initiated Facial Recognition (OIFR) which is where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis.

3.2 Terminology

3.2.1 Within EP and throughout EP's LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition: -

3.2.2 Adjudication.

A human assessment of an alert generated by the Live Facial Recognition (LFR) application by an LFR engagement officer (supported, as needed by the LFR operator) to engage and further confirm identification with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject, system and environmental factors.

3.2.3 Administrator

A specially trained person who has access rights to the LFR application to optimise and maintain its operational capability.

3.2.4 Alerts

An alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the watchlist and returns a comparison (similarity) score above the threshold.

3.2.5 True Alert

A true alert is determined when the probe image is the same as the candidate image in the watchlist.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.2.6 Confirmed True Alert

Following engagement, a confirmed true alert is determined when the engaged individual is the same as the person in the candidate image in the watchlist.

3.2.7 True Positive Identification Rate (TPIR)

It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated). This is also referred to as the true positive identification rate.

3.2.8 False Positive Identification Rate (FPIR)

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement. (The false alert rate is one of the two measures relevant to determining application accuracy).

3.2.9 Confirmed False Alert.

Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

3.2.10 False Alert Rate

The number of individuals that are not on the watchlist who generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition. This is also referred to as false positive identification rate.

3.2.11 Application Accuracy

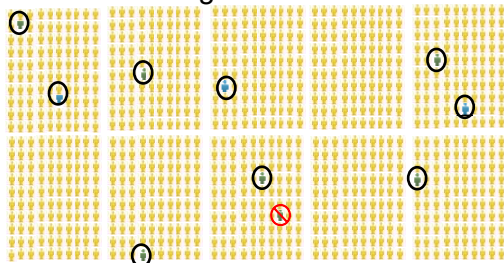
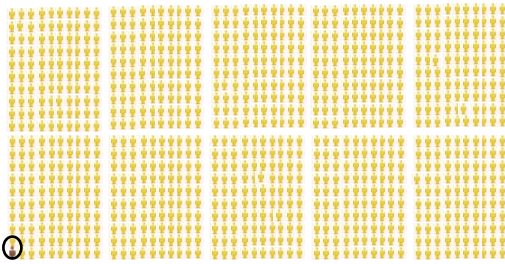
Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the 'True Recognition Rate' and the 'False Alert Rate'. This is further explained below. The example given has been simplified to demonstrate the concept, but note that the metrics have been calculated in accordance with the agreed scientific method as set out by the International Organisation for Standardisation:

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

	True Recognition Rate	False Alert Rate
What is it?	It is the total number of times an individual(s) on a watchlist is known to have passed through the Zone of Recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the Zone of Recognition. This is regardless of whether an alert is generated by the LFR application or not.	Is the number of individuals that are not on the watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
Worked Example	The True Recognition Rate would be  90% if 10 people on the watchlist each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people (with no alert being generated against the 10th person).	The False Alert Rate would be 0.1%, if for every 1,000 people that passed the LFR system, an Alert was generated against one person who was not on the watchlist. 

3.2.12 Authorising Officer (AO)

The officer (usually holds the rank of Superintendent or above) who provides the authority for deployment of LFR.

3.2.13 Biometric Template

A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

3.2.14 Blue Watchlist

A watchlist comprises known persons that can be used to test system performance, for example, police officers / staff may be placed on a blue watchlist and 'seeded' into the crowd who walk through the zone of recognition during a deployment.

3.2.15 Candidate Image

Image of a person from the watchlist returned because of an alert.

3.2.16 Deployment

Use of an LFR application as authorised by an AO to locate those on an LFR watchlist at a designated location.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.2.17 Deployment record.

An amalgam of the LFR application, the written authority document and the LFR cancellation report. This sets out the details of a proposed deployment including – but not limited to:

- a. location
- b. dates and times
- c. deployment and watchlist rationale
- d. legal basis
- e. necessity
- f. proportionality
- g. safeguards
- h. watchlist composition
- i. authorising officer
- j. resources
- k. relevant statistics
- l. outcomes
- m. summary of any issues
- n. threshold setting.

3.2.18 Engagement

An officer communicating with a member of the public as a result of an alert.

3.2.19 Environmental Factors

An external element that affects LFR application performance, such as dim lighting, glare, rain, mist.

3.2.20 Faces per frame.

A configurable setting that determines the number of faces that can be analysed by the LFR application in each video frames.

3.2.21 Facial Recognition Technology (FRT)

This technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database and generates possible matches. This is based on digital images (either still or from live camera feeds).

3.2.22 False Negative

Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are several reasons false negatives occur; these include application, subject and environmental factors, and how high the threshold is set.

3.2.23 Gold Commander

Is the strategic commanding officer who assumes overall command and has ultimate responsibility and accountability for the Deployment. (They are responsible and accountable for the policing operation/event and determine the strategic objectives and separate to other force wide daily gold commanders).

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.2.24 Live Facial Recognition (LFR)

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist to locate persons of interest by generating an alert when a possible match is found.

3.2.25 LFR Engagement Officer

An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR deployment.

3.2.26 LFR Operator

An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

3.2.27 LFR System Engineer

A person whom EP deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of the Essex Police LFR system.

3.2.28 Person(s) of Interest

A person on a watchlist

3.2.29 Possible Match

A person returned because of the probe and candidate image being of sufficient similarity above the threshold.

3.2.30 Probe Image

A facial image which is searched against a watchlist.

3.2.31 Recognition Time

The average time from when a face appears in the zone of recognition of the camera to when the LFR application generates an alert.

3.2.32 Retrospective Facial Recognition (RFR)

A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database to identify them.

3.2.33 Silver Commander

The officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander. (The silver commander develops, commands, and coordinates the overall tactical response of an operation, in accordance with the strategic objectives set by the gold commander).

3.2.34 Similarity Score

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

Is a numerical value indicating the extent of similarity between the probe and candidate image, with a higher score indicating greater points of similarity.

3.2.35 Subject Factor

A factor linked to the individual, for example, demographic factors or physical features or behaviours for example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.

3.2.36 System Factor

A factor relating to the LFR application such as the algorithm.

3.2.37 Threshold

The configurable point at which two images being compared will result in an alert. The threshold needs to be set with care to maximise the probability of returning true alerts whilst keeping the false alert rate to an acceptable level.

3.2.38 Urgency

In the context of authorising an LFR deployment, a deployment that is related to an: Imminent threat-to-life or serious harm situation; and/or intelligence / investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action.

3.2.39 Watchlist

A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (from the reference image database) and will have been created specifically for the LFR deployment. The reference images are sourced from Athena, Missing person database (COMPACT) and Images provided by public with consent.

3.2.40 Zone of Recognition

A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.

3.3 Legislative Compliance

3.3.1 This document has been drafted to comply with the principles of the Human Rights Act 1998. It pays particular attention to the duties of the force regarding privacy and the rights to assembly, thought and expression.

3.3.2 Equality and Diversity duties and issues have been considered, and this is reflected in the Equality Impact Assessment that is provided alongside this document.

3.3.3 As with all policies, the duties, and obligations of the force regarding Data Protection, Freedom of Information and Health and Safety matters have been

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

considered and complied with along with The College of Policing's Authorised Professional Practice (APP) on Facial Recognition Technology.

3.3.4 Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. Essex Police is conscious that the use of LFR has been the subject of much debate. Areas subject to particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.

3.3.5 It is therefore incumbent on Essex Police to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will be in line with Human Rights requirements and Public Sector Equality Duty. This will help ensure that public trust and confidence is not eroded by the use of LFR.

3.3.6 Essex Police will adopt similar safeguards to other forces utilising LFR technology. These safeguards, are as follows:

3.3.6.1 Each Deployment must be carefully designed and have clear, documented objectives.

3.3.6.2 The watchlist for any deployment will be primarily restricted to individuals who are wanted for offences linked to the purpose deployment and likely to be in that deployment.

3.3.6.3 There may be an intelligence/evidence case to include a watchlist of individuals who are at risk of serious harm. This will however only be those that are medium or high risk.

3.3.6.4 In general, deployments will not include watchlists of victims or witnesses. The Authorising Officer (AO) would only ever consider inclusion if the same test as point 3.3.6.3 above was met in terms of medium or high risk of serious harm.

3.3.6.5 The AO must ensure that their assessment and authorisation clearly articulates legality, necessity, and proportionality.

3.3.6.6 Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any concerns the public may have with regards to how their human rights are engaged.

3.3.6.7 The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the Deployment are appropriately trained, briefed, and accountable. Also, that equipment will be used correctly, and that

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

those involved in the Deployment mitigate against inappropriate responses to LFR application Alerts.

3.3.7 The AO must also consider how the Deployment of LFR may impact on communities, and how the rights of everyone whose image is likely to be captured by the LFR application have been considered, and what safeguards are in place to protect them. The software is designed to disregard anyone who is not on the watchlist within under a section.

3.3.8 Essex Police is not only concerned with developing and implementing precision policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. Essex Police will implement a robust governance process to review the effectiveness and impact of its LFR deployment. Essex Police will focus on delivering transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from Essex communities as part of an ongoing process.

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

3.4 Strategic Intention, Objectives and Use Case

3.4.1 LFR Deployments must be run under a Written Authority Document that complies with the following strategic intentions and operational objectives.

3.5 Strategic Intentions

Essex Police will:

3.5.1 use overt LFR technology in a responsible and proportionate way to locate offenders in accordance with Essex Police' common law policing powers. This includes targeting those wanted for criminal offences, those who pose a risk of harm, those wanted by the courts and potentially members of the public who are at serious risk of harm.

3.5.2 EP will comply with the common law and statutory safeguards in delivering its policing operational duties and rely on the common law to discharge a number of its duties. LFR can assist with Essex Police duties to protect life and property, preserve order, and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security. This includes targeting those wanted for offences. It also includes using LFR technology to protect the public and reduce crime, and

3.5.3 strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep Essex safe.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.5.4 build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns, maximising transparency and maintaining the ongoing testing and exploration of the algorithm; and

3.5.5 maintain good governance through a command structure that incorporates strategic, operational, and technical leads for the deployment of LFR, with clear decision making and accountability; and

3.5.6 ensure that the deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and Essex Police LFR Documents; and

3.5.7 transparently identify, manage, and mitigate any impact on public trust and confidence; and

3.5.8 be recognised as a progressive, responsible, and ethical organisation; and

3.5.9 use in an equitable manner to ensure trust and confidence across all communities

3.6 Operational Objectives

Essex Police will:-

3.6.1 use LFR technology to enable Essex Police to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities; and

3.6.2 adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight is active and involved, with the officer retaining full control and making the decision on whether to take action; and

3.6.3 engage with and provide reassurance to communities, listening and responding to concerns; and

3.6.4 continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

3.7 Technological Objectives

Essex Police will: -

3.7.1 ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.7.2 provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other imprisonable offences; and

3.7.3 look to technological improvements whilst keeping the EP LFR SOP under review. Where appropriate we will trial against alternative providers of facial recognition software and hardware. This helps to ensure that the best possible service is sought, and we can proactively develop improved working methodologies and accuracy. The outcomes of any parallel trial will be captured with the same key performance metrics that are gathered when deploying LFR to ensure the findings are suitable for direct comparison and analysis. All previously detailed retention periods will remain unaffected.

3.8 Use of LFR

This guidance relates to the use of LFR in an overt capacity to help EP protect the public. EP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool.

3.8.1 LFR helps EP use its resources more efficiently. EP considers that LFR is better than humans at recognising persons from a large dataset (generally hundreds to low thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to EP.

3.8.2 The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies. (It is acknowledged that considerations regards data protection should not be considered as an absolute barrier to information sharing).

3.8.3 Locations for the deployment of LFR will be kept under strict review, with LFR being deployed into areas where it has the greatest potential to assist EP in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why a location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other EP LFR Documents.

3.8.4 Given that LFR requires a member of EP personnel to review every Alert in real-time for a decision as to whether any further action is required, EP will always deploy LFR in a way that is operationally effective and allows EP to act on any Alerts as they are generated. LFR will not be used indiscriminately.

3.9 Overview of LFR Deployment Processes

End-to-End Process

3.9.1 The end-to-end process of an LFR Deployment can be summarised as follows:-

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.9.1.1 LFR law enforcement purpose identified, safeguards considered, Deployment authorised, and Watchlist selected.

3.9.1.2 Notification of Deployment, and signage deployed. The public will be given five working days' notice and engagement prior to deployment. Unless there is a significant operational reason for that period to be reduced.

3.9.1.3 As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist.

3.9.1.4 If a possible match is found in a Watchlist, the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the Watchlist are presented to the LFR Operator / LFR Engagement Officer for human review.

3.9.1.5 The LFR Operator / LFR Engagement Officer will consider the Alert, noting the system, subject and environmental factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is engaged.

3.9.1.6 Cancellation of authority for the LFR Deployment and post-Deployment evaluation.

3.9.1.7 EP LFR SOP provides a greater level of detail about the processes involved in the deployment of LFR by EP. A flowchart summarising LFR deployment will be provided for frontline staff in due course.

Key Points:

- a) LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are on a Watchlist.
- b) The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area.
- c) The quality and resolution of images (both those in the Watchlist and those from the video cameras) are of vital importance and must be carefully considered.
- d) The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.
- e) It is important to balance the objectives of the operation with the size of the Watchlist and the available resource to respond to Alerts. If the objectives are too broad and/or the Watchlist is too large, the amount of resource required to respond to Alerts may be prohibitively high.

3.10 Policing LFR Deployments Effectively

There must be sufficient appropriately trained resource deployed to be able to respond to Alerts. This is important to ensure that the LFR application, and the data processed by it, is being effectively used.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.10.1 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of true positive identification rate (TPIR) and Recognition Time, and the probability of people from the Watchlist being observed by the camera (i.e. occlusion) and their likely presence are all matters that must be considered when deciding what resources should be available.

3.10.2 It is also vital that EP is transparent in its use of LFR under this guidance. As well as using signage, the provision of sufficient policing resource will allow officers to answer questions that the public may have.

3.11 Governance, Oversight and Impact Assessments

3.11.1 Following consultation the following stipulations have been proposed and accepted by EP:-

- a. The overall benefits to the public must be balanced with public confidence of our use of LFR.
- b. It can be evidenced that the technology itself will not result in unacceptable gender or racial accuracy variance into policing operations. This is supported by the two academic and scientific studies into the accuracy of the algorithm by Cambridge University and the NPL.
- c. Each Deployment must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific policing purpose.
- d. LFR Operators are trained to understand the risks associated with use of the LFR application, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions.
- e. EP 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 considering guidance from the Surveillance Camera and Biometric Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

3.12 Governance Framework

EP LFR documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:

- a. Pre-Deployment;
- b. Operational Deployment;
- c. Post-Deployment.

3.13 Pre-Deployment

Authority to deploy LFR is an operational one, where the EP Authorising Officer (AO) rank is set at Superintendent. In exceptional cases of urgency, an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the deployment of LFR.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.13.1 Where an officer below the rank of Superintendent provides the authority, a Superintendent must be informed as soon as practicable. It is for the Superintendent to then authorise the deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.

3.13.2 Prior to AO authorisation and the deployment of LFR in public spaces, several documents must be completed. In some instances, the AO may seek to consult with the Chief Officer regarding the specific circumstances of a particular deployment if it falls outside of normal deployment parameters, for example the use of an image of a child under the age of 13yrs, circumstances in line with the circumstances described at 13.8, 3.10, 3.28 of the D2701 Procedure Document. This allows the Chief Officer the opportunity to consider the circumstances and either veto the deployment or ask the AO to consider any mitigation that may be required to address the concerns at hand.

3.13.3 The AO must notify the Essex Police, Fire, and Crime Commissioner (or designated staff member) prior to any deployment.

3.13.4 The EP Data Ethics Committee are an independent source of advice. Their terms of reference include the provision of advice and independent oversight of EP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework They have supported and consulted on the preparation and development of LFR process.

3.13.5 Several specific EP documents and records need to be completed in support of each deployment. These are set out below:

EP LFR Deployment Specific Documents and Records	
LFR Application	Sets out the details of a proposed deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.
Written Authority Document	The AO's written authority provides a decision-making audit trail demonstrating how the AO has considered the legality, necessity, and proportionality of the deployment of LFR, the safeguards that apply and the alternatives that were considered but deemed to be less viable to realise the policing purpose. The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained because of the LFR Deployment. The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

LFR Deployment Record	Records details of where and when a deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.
Assessments	These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Biometrics and Surveillance Camera Commissioner's Self-Assessment. These documents need to be considered by the decision-maker when authoring a deployment to ensure they are sufficient to address the issues arising from the proposed deployment. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the deployment is not only necessary, but also proportionate to the policing purpose.
Deployment Logs	Logs completed in the planning and execution of an LFR deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.

3.13.6 Several other specific EP documents pertaining to each EP LFR Deployment have been completed centrally. These are set out below:

EP LFR Documents and Records	
EP Data Processing – Appropriate Policy Documents	EP policy on the processing of data pursuant to the Data Protection Act 2018 and UK General Data Protection Regulation relating to LFR.
EP Legal Mandate	Outlines the legal considerations to be addressed in order to use LFR.
EP Training Protocols	Provides the necessary training to ensure those involved in authorising and deploying LFR are familiar and implement the considerations relevant to its lawful, ethical and appropriate use.

3.14 Operational Deployment

Arrangements must be made to accurately record and log the dates, times, and location of the deployment.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.14.1 The Silver Commander must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the deployment. The Silver Commander needs to be content:

- a) that the use of the LFR remains necessary and proportionate for the policing purposes identified in the Written Authority Document; and
- b) that the safeguards identified in the written approval remain effective; and
- c) that the level of officer support committed to the deployment is enabling Alerts to be responded to effectively; and
- d) that the Subject, System and Environmental Factors are such that the use of the LFR application remains effective for realising the policing purpose identified in the written approval.

3.14.2 Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples may include occlusion resulting in those sought not being presented to the camera in cases of high crowd flow, adverse weather / lighting conditions or operational events changing the resources needed in the area. The Silver Commander must be empowered and have absolute discretion to suspend or terminate the deployment. Further details are provided within the LFR SOP.

3.14.3 In any event the Silver Commander must conduct and record a review of the activity at suitable intervals during the deployment. The timing and frequency of reviews is determined by the Silver Commander. A suitable period should be determined in the context of the deployment. This review should address the continued legality, necessity, and proportionality of the deployment, as well as providing some analysis on LFR application performance and the engagements undertaken.

3.15 Post-Deployment

The use of LFR should be subject to debrief and review. This will help ensure that future deployments reflect learning identified from each deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the deployment.

3.15.1 The original authority specifies times and dates when the technology can be deployed. Once this period has lapsed then the authority is cancelled and requires an extension or new authority. If the deployment is stopped or cancelled prior to deployment then the AO is notified.

3.15.2 The outcome of LFR deployments is subject to evaluation, which in turn should feed into oversight and scrutiny processes. This will include quarterly assessment of positive intervention data focussing on crime type, outcomes and specialist characteristics such as age, gender and ethnicity.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.15.3 Post-Deployment, EP must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with EP LFR documents. This includes that: -

- a) where the LFR system does not generate an Alert that a person's biometric data is immediately automatically deleted; and
- b) the data held on any medium used to import the watchlist is deleted as soon as practicable, and in any case, within 24 hours following the conclusion of the deployment so it encompasses both egress and a USB stick.

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

3.15.5 All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-

- a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- b) in accordance with EP's complaints / conduct investigation policies.

3.16 Oversight Bodies and Regulatory Framework

Within EP, the senior internal oversight body for LFR is the FR Strategic Board. In addition, The Essex PFCCs office will also provide an external oversight and scrutiny perspective. The Facial Recognition Delivery Board provides and explores current processes and governance of the deployment of FR technology and reports into the Strategic Board.

3.16.1 EP LFR Legal Mandate sets out the legal framework for EP use of LFR technology, whilst EP LFR Policy Document and EP LFR Procedure support implementation.

3.16.2 Nationally, the NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.

3.16.3 Further oversight opportunities may arise in relation to the Joint National Biometric Strategic Board. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the Information Commissioners Office, the Biometrics and Surveillance Camera Commissioner.

More detail on these roles:-

- a) Biometrics and Surveillance Camera Commissioner (SCC); The Biometrics and Surveillance Camera Commissioner's role is to encourage compliance with the surveillance camera code of practice. Their key responsibilities is to:
 - keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints.
 - decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984)

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

- review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints
- provide reports to the Home Secretary about the carrying out of his functions
- encourage compliance with the Surveillance Camera Code of Practice
- review how the code is working
- provide advice to ministers on whether or not the code needs amending.

See [About us - Biometrics and Surveillance Camera Commissioner - GOV.UK \(www.gov.uk\)](https://www.gov.uk/about-us-biometrics-and-surveillance-camera-commissioner)

- a) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Protection Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018.

See [Information Commissioner's Office \(ICO\)](https://ico.org.uk/)

3.17 Public Engagement

3.17.1 Public engagement must be supported using online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of deployments. At and around the location of deployments, notices providing information, including details of the Privacy Notice, should be distributed and feedback via email should be sought.

3.17.2 Operational briefings delivered to officers and stakeholders prior to deployments should promote openness with the public and transparency about the use of LFR. Officers should be encouraged to engage with the public to increase awareness of how LFR helps keep the public safe and how it helps bring offenders to justice. It is also helpful for officers to be in possession of information leaflets that can be handed out to the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.

3.17.3 Key stakeholders, including the PFCC's Office, may be invited to observe the planning and deployment of LFR although it must be noted that the deployment is an operational matter.

3.18 In Advance of Deployments

In advance of deployments EP will ensure that:-

- a) LFR Deployments are notified to the public using EP website and other appropriate communication channels (including social media); and
- b) LFR awareness raising measures (e.g. signs and/or leaflets) are prepared to support LFR deployment in line with EP LFR Procedure; and
- c) literature is prepared for persons who may be engaged (to include information outlined within a privacy notice); and

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

- d) Officers are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a Constable in uniform to compel a person to remove anything that conceals their identity; and
- e) external engagement is considered in discussion with EP LFR team. It may be appropriate to pursue engagement opportunities with several stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

3.19 During Deployments

During deployments ensure that: -

- a) awareness raising measures are used in line with the EP LFR Procedure to ensure that the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed; and
- b) notices with a brief explanation and reference to EP website are available to hand out to the public on request; and
- c) information is offered to persons engaged by officers in accordance with the policy referred to above.

3.20 After Deployments

After deployments ensure that: -

- a) information about the deployment, including location, time, date, number of alerts, engagements, arrests, and any other information considered helpful and suitable for disclosure, is published on EP website. Care must be taken to ensure that no personal data is published.
- b) external engagement is considered in discussion with EP LFR team. Again, it may be appropriate to pursue engagement opportunities with several stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity; and
- c) Ongoing internal assessment of benefits of performance of LFR technology will take place.

3.21 Watchlist Considerations

3.21.1 Image Quality

The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. The best images are those that follow a custody or passport style image that conforms to the NPIA 'Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.21.2 The EP Legal Mandate provides commentary on the legal considerations relevant to compiling a Watchlist in a lawful way. This means that we ensure we hold the Watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes. The watchlist will be compiled, in its final form, no more than 24 hours before the first deployment.

3.21.3 Key points include ensuring the Watchlist is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. EP LFR SOP provides practical guidance on how to follow EP LFR Documents, including EP Legal Mandate.

3.21.4 The size of the Watchlist is relevant to the level of resource that should be available to a deployment. There must be sufficient resource available to manage the alerts generated by the LFR application.

3.21.5 As explained in section 3.8 (LFR Overview), Watchlist composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment. How great that likelihood needs to be will vary between cases for inclusion, but in any case, should be considered against a number of factors. This means that an AO may deem it necessary and proportionate to authorise the inclusion of people to be included in a Watchlist, even though there may not be specific intelligence to say where in EP they might be found. Factors for consideration in this respect include:

- a) Severity of offence in question; this will often be relevant to the level of urgency associated with locating and arresting an individual. Many individuals change their behaviour, including the places they reside and frequent when they know that they are wanted for a serious offence.
- b) Risk: The level of risk associated with an individual or the offence type sought, whether that risk is to the public or themselves;
- c) Deployment location: the specific characteristics of the deployment location may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the Watchlist. Areas around transport hubs have a lot of people transiting from place to place.

3.22 Governing the Watchlist

3.22.1 The systems used to generate the Watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

3.22.2 EP LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose. The search carried out in relation to the creation of the watchlist will be

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

retained securely for three months to ensure correct scrutiny and examination can be conducted if required.

3.22.3 The watchlist will be downloaded primarily using a secure file sharing platform to minimise the risk of data hacking. With a backup option of downloading to a secure data stick. Where, for technical reasons, this is not possible, the data stick will be subject to a physical security process that will ensure it is stored securely and when it is not stored it will be in the physical possession of a police officer.

3.23 Governing the Watchlist

3.23.1 The systems used to generate the Watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

3.23. EP LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose. The search carried out in relation to the creation of the watchlist will be retained securely for three months to ensure correct scrutiny and examination can be conducted if required.

3.24 Addressing Disproportionality

3.24.1 EP does not create or routinely retain a breakdown of race, gender or any other protected characteristic of persons on a Watchlist as standard practice. This mirrors the approach taken with most policing tools used by EP. The exception here is for inclusion of under 18's and under 13's as previously detailed.

3.24.2 The deployment of LFR is driven by EP policing priorities, intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose that determines the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, there are realistic prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.

3.24.3 The routine retention of data relating to protected characteristics would mean EP holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a Watchlist. Data is kept relating to positive interventions. This includes the crime type and outcome together with specialist characteristics such as age, gender and ethnicity

3.24.4 EP recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. The testing carried out by Cambridge University and the National Physical Laboratory (NPL) provides the assurances that

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

the algorithm and relevant threshold settings are set within the requirements outlined by legislation and national protocol.

3.24.5 EP also uses the results of academic equitability testing of the LFR system where necessary. The necessity and frequency are determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms. This includes exploring not only previous testing but post-initial deployment testing.

3.24.6 When equitability tests are conducted, no biometric data belonging to members of the public is retained for the purpose of the tests. As part of these tests, a human operator monitors and records perceived gender, ethnicity, age and any other relevant protected characteristics, of persons passing through the Zone of Recognition during an LFR Deployment.

3.24.7 EP has several measures to guard against a System Factor (system bias) affecting the generation of Alerts. For example, being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:-

- a) those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and environmental Factors throughout the Deployment. Should concerns arise that the LFR system is not performing correctly, the Silver Commander will halt the Deployment where necessary; and
- b) for the purpose of facilitating post-Deployment reviews, Alerts are retained for up to 24 hours. It provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in place for the Deployment,
- c) in the event post-Deployment reviews identify an area of concern, EP may undertake further equitability testing where this appears necessary.
- d) a quarterly assessment of positive intervention data, from alert to intervention, focussing on crime type, outcomes and specialist characteristics such as age, gender and ethnicity.

3.24.8 Following evaluations by NPL, Cambridge and an assessment by the NPCC Chief Scientific Officer it is determined that the algorithm deployed at a threshold of 55 maintains equitable performance while achieving a false positive rate significantly below the national and legal requirement.

3.25 False Positive Identification Rate (FPIR) / True Positive Identification Rate (TPIR)

3.25.1 There are two types of False Positive Identification Rate (FPIR) measurements. The first is the System FPIR, which is the number of False Alerts generated as a proportion of the total number of subjects processed by the LFR application. The second is the Operational FPIR, which is calculated in the same way, but is measured after the LFR Operator has reviewed the output from the LFR application and dismissed LFR application Alerts assessed by the LFR Operator as false.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

3.25.2 All the True Positive Identification Rate (TPIR) and FPIR metrics should be recorded and reported. Operational experience to date suggests that in most scenarios the FPIR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the FPIR is greatly affected by the number of subjects processed by the LFR application, and to a lesser extent, the size of the Watchlist. This is a key reason why the number of persons included on the Watchlist needs to be kept as small as possible, whilst still meeting operational objectives.

3.25.3 It should also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TPIR and FPIR. The Threshold needs to be set with care so as to maximise the probability of returning correct Possible Matches, whilst keeping the number of False Alerts to acceptable levels. Algorithm testing conducted by Cambridge University and the NPL, in addition to an assessment by the NPCC Chief Scientific Officer has determined that a deployment threshold of 55 maintains equitable performance balanced with achieving a false positive rate significantly below the national and legal requirement.

3.26 Recognition Time

3.26.1 A third important metric is the Recognition Time (RT). Note that the actual amount of time taken to act on an Alert will always be longer than the RT as additional time is needed for the LFR Operator to assess the Alert and to pass to an LFR Engagement Officer to then make a final decision on whether to Engage or not.

3.26.2 The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

3.27 LFR Guidance Summary

3.27.1 This guidance relates to the operational use of LFR, and the governance and oversight regimes necessary to support Deployment.

3.27.2 It is strongly advised that officers and staff adhere to the guidance as this will help ensure that EP use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.

3.27.3 It is recognised circumstances may arise where for valid reasons, a decision is taken that it is necessary to things slightly outside of this guidance. This guidance will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are at odds with some aspects of this guidance, it is essential these decisions are fully documented,

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

together with detailed rationale, and that the relevant decision-making features within debrief and evaluation processes.

4.0 Implications of the Policy

4.1 Finance / Staffing / Training / Other

4.1.1 The CCTV vans and LFR software have been purchased by Essex Police who now own the facility. Deployments will be subject of the tasking process and relevant agreed funding if required.

4.1.2 Staffing primarily will be provided by the Operational Policing Command who have ownership and control of the CCTV vans and LFR software. All authorities will be assessed and authorised by qualified Authorising Officers (AO's) within the Serious Crime Directorate (SCD)

4.1.3 Training has been provided by the LFR provider as part of the tender process. OPC have been trained in the use of LFR software and can further train staff if or when there is a requirement. ONLY staff trained in use of the LFR software will be able to operate it.

4.2 Risk Assessment(s)

4.2.1 Compliance with this Policy is mandatory, there are no specific health and safety considerations for police officers or police staff when following this procedure.

4.2.2 There are risks associated with deployment of LFR technology when considering the public rights under the Human Rights Act. If this policy and associated procedure is followed accordingly then at every stage of proceedings and deployment the public's rights will be considered and assessed accordingly in line with the college of Policing APP and relevant case law.

4.2.3 The risk in non-compliance with Human Rights legislation could lead to a negative impact on public confidence and trust on the communities we serve. This could also have legal implications on the force.

4.2.4 General Data Protection Regulation (GDPR) and Data Protection – All potential risks in relation to DPIA have been documented within the DPIA 1&2. Non-compliance of GPDR would mean that we would breach legislation and be vulnerable to legal challenge.

4.2 Equality Impact Assessment

4.2.1 This policy has been assessed and graded as High Risk

4.2.2 Consultation has taken place with an independent ethics panel who are supportive of concept, testing and proposed deployment criteria.

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

4.2.3 EIA – February 2026

5.0 Consultation

The following have been consulted during the formulation of this document:

- Data Protection
- IT
- Legal
- Information management
- Information security
- Finance
- Ethics committee
- Local IAGs
- Unison
- Police Federation
- Essex Diversity and Inclusion Team
- Health & Safety
- Head of Operational Change
- PSD D/Superintendent
- Risk
- Policy
- Superintendents Association
- Strategic Force Crime & Incident Registrar
- DPO/Temp Head of Info Management
- Head of Operational HR
- Support Network Chairs and Vice Chairs
- Specials Command Essex
- Essex Diversity and Inclusion Team
- Head of Continuous Improvement
- Head of the Control Centre

6.0 Monitoring and Review

This policy will be reviewed annually.

This policy is owned by Detective Superintendent Stephen Jennings. They are responsible for ensuring this policy is regularly reviewed and updated in line with any national guidance and legislative changes.

7.0 Related Force Policies or Related Procedures

- EP Live Facial Recognition Procedure
- EP Live Facial Recognition Data Protection Impact Assessment (DPIA)
- EP Live Facial Recognition Legal Mandate
- EP Live Facial Recognition Equality Impact Assessment
- EP Live Facial Recognition Training Documents and User Guides

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

7.1 Data Security

Essex Police have measures in place to protect the security of your data in accordance with our Information Management Policy - [W 1000 Policy – Information Management](#).

7.2 Retention & Disposal of Records

Essex Police will hold data in accordance with our Records Review, Retention & Disposal Policy – [W 1012 Procedure/SOP - Records Review, Retention and Disposal](#).

We will only hold data for as long as necessary for the purposes for which we collected. Victims/public should be reminded that Essex Police take the protection of personal data seriously as described in the privacy notice <https://www.essex.police.uk/hyg/fpnessex/privacy-notice/>.

8.0 Other Source Documents, e.g., Legislation, Authorised Professional Practice (APP), Partnership Agreements, Force Forms (if applicable)

Acronyms used in LFR.

AO	Authorising Officer
BC	Biometrics Commissioner
CCTV	Closed Circuit Television
CIA	Community Impact Assessment
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EIA	Equality Impact Assessment
FAR	False Alert Rate
FR	Facial Recognition
FoIA	Freedom of Information Act
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
ISO	International Standards Organisation
LEA	Law Enforcement Agency

POLICY – Live Facial Recognition

Number: D 2700

Last Updated: 17th March 2026

Version 4 – March 2026

LFR	Live Facial Recognition
MOPI	Management of Police Information
SWP	South Wales Police
EP	Essex Police
NPCC	National Police Chiefs' Council
NPL	National Physics Laboratory
RT	Recognition Time
SCC	Surveillance Camera Commissioner
SCCSA	Surveillance Camera Commissioner's Self-Assessment
SOP	Standard Operating Procedure
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition

Policy Author: Detective Superintendent 42000494 Stephen Jennings

Policy Owner: Detective Superintendent 42000494 Stephen Jennings

Cancellations: N/A