

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

1.0 Summary of Changes

- 1.1 Changes to the stages of deployment since the inception of the LFR webpage and introduction of CHARTER (3.5.1)
- 1.2 Additional comments to show that LFR applications are made on the CHARTER system (3.5.3)
- 1.3 Change of wording to the period of time which a single consecutive application can be made. (3.5.4)
- 1.4 Wording included to outline the point in which an authority ceases and is cancelled (3.6.1)
- 1.5 Addition of the changes to the software to increase the software to only allow images that reach 100 pixels to prevent future false positives (3.15.2 & 3.35.1)
- 1.6 Inclusion of 'Medium Risk' mispers to options for watchlist creation. This was declared appropriate by the High Court in recent judicial proceedings. (3.22 & 3.23)
- 1.7 Addition of the four-stage approach following a positive alert (3.38.4)
- 1.8 Response to the Cambridge and NPL Reports
- 1.9 Quaterly reviews of the positive interventions

2.0 What this Procedure is about:

- 2.1 This procedure explains the standard procedures to be adopted when planning for, using, and reviewing the use of Live Facial Recognition.
- 2.2 This LFR procedure document provides Essex Police personnel with advice on the overt use of LFR in a legally compliant and ethical manner to enable Essex Police to achieve legitimate policing aims.
- 2.3 This procedure document has been written with consideration to the views of the Information Commissioner, Biometrics and Surveillance Camera Commissioner, national guidance, academic based testing and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).
- 2.4 This procedure is particularly aimed at (this list is non-exhaustive):
 - All operational officers and staff, and their supervisors involved in the planning and deployment of LFR.
 - All officers and staff involved in any subsequent investigation resulting from the operational deployment of LFR technology.
 - All authorising officers (AOs)
 - All officers applying for the deployment of LFR.
 - The operational command team for LFR deployment (Gold, Silver and Bronze)
 - LFR operators, LFR engagement officers and LFR system engineers.

Compliance with this procedure and any governing policy is mandatory.

3.0 Detail the Procedure

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

3.1 Terminology

This procedure focuses exclusively on LFR. Terminology relating to LFR is defined in the Essex Police LFR Policy Document

3.2 Aim and Scope of Procedure

This procedure aims to:

- Provide Essex Police personnel with information about the strategic and operational objectives of the overt use of LFR.
- Provide Essex Police personnel with guidance on the deployment of overt LFR technology by Essex Police in spaces accessible to the public to meet Essex Police's objectives for LFR.
- Establish the governance structure for the deployment of LFR, ensuring that Essex Police use of LFR is appropriately governed and legally compliant.
- Provide an overview of LFR technology and advise on practical issues such as camera selection and placement to obtain the best performance from the LFR system.

3.3 Legislative Compliance

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.

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

As with all policies, the duties, and obligations of the force regarding Data Protection, Freedom of Information and Health and Safety matters have been considered and complied with along with The College of Policing's Authorised Professional Practice (APP) on Facial Recognition Technology.

3.4 Strategic Objectives

LFR deployments must comply with the following strategic objectives:

- Use overt LFR technology in a responsible and proportionate way to locate offenders in accordance with Essex Police's common law policing powers. This includes targeting those wanted for criminal offences, those who pose a risk of harm and those wanted by the courts.
- Use LFR 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.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- Strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons including missing people and children, and to keep Essex safe.
- Build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns and maximising transparency.
- 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.
- 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.
- Transparently identify, manage, and mitigate reputational and organisational risk to Essex Police.
- Be recognised as a progressive, responsible, and ethical organisation.

3.5 Authority to Deploy LFR

3.5.1 There are ten stages of deployment which consist of the following:

- STAGE 1 - Departmental/LPA identification of potential LFR deployments
- STAGE 2 - Check availability of LFR vans via the LFR webpage.
- STAGE 3 - Local or Force Tasking bid if required.
- STAGE 4 - Complete LFR Application on CHARTER software.
- STAGE 5 – CAB will quality assure the application and send to the authorising officer.
- STAGE 6 - Authorising Officer assessment of application and authority.
- STAGE 7 - Public notification of deployment via media department (five working days prior)
- STAGE 8 – Notification of deployment to the PFCC and ACC, Serious Crime Directorate.
- STAGE 9 - Populating the watchlist (including PND searches)
- STAGE 10 - Deployment of LFR technology

3.5.2 In normal circumstances the authorising officer who authorises a LFR deployment should not be below the rank of Superintendent. It is preferred but not necessary for this Superintendent to be an accredited Authorising Officer. This authorisation should be in writing.

3.5.3 The EP LFR Application / Authority Document recognises that the intelligence case for the use of LFR may give rise to a single deployment, or a need for a series of deployments within a time-limited period. All applications are to be written and authorised within the CHARTER system software.

3.5.4 In Essex Police an Authorising Officer may authorise the use of LFR based on one application for a period of up to 7 consecutive days. An authority can be granted

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

for separate days over a period of time if the intelligence case and legitimate Policing aim is met.

3.5.5 The application combined with the authorising document provides for a baseline of safeguards to ensure that the need for the deployment and the currency of the watchlist continues to be maintained with due oversight.

3.5.6 Should the need to deploy continue beyond 7 days, a further EP LFR Application will be submitted, and a further authority would be granted if, in the AOs view the conditions for deployment continue to be met.

3.5.7 This approach ensures that the use of LFR is time limited but allows an operationally effective way to plan for and deliver LFR as part of wider EP crime-fighting strategies.

3.5.8 A Chief Officer does not provide authority for LFR deployment. However, 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 3.8, 3.10, 3.28. 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.

3.5.9 The AO must notify the Essex Police and Fire Commissioner (PFCC) or a designated deputy prior to any deployment.

3.5.10 Where the AO is not immediately able to provide their authority in writing and the request is urgent, such authority may be given verbally. The time of this verbal authority must be recorded by the applicant and the AO. Written authority must then be recorded as soon as it practicable.

3.5.11 Urgent deployments are defined as those where a delay in deployment in order to complete a written application and authority documents would place people or property at serious risk of harm or be a risk to national security; or

3.5.12 An intelligence or investigative opportunity with limited time to act, the seriousness of which and the benefit of deployment justifies urgent action.

3.5.13 The AO must consider and document the below:

- The legitimate policing aim of the deployment and the legal powers that are being relied upon to support the deployment and
- That the AO is satisfied that the deployment complies with this procedure, Essex Police policy and other relevant LFR documentation (including legal mandate and EIA) and
- How and why the deployment is necessary (not simply desirable) and is proportionate to achieve the legitimate aim of the deployment. The AO must

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

give due consideration to the Human Rights Act 1998 in respect of this determination and

- Articulate that the processing of sensitive personal information is strictly necessary for a law enforcement purpose as defined by the Data Protection Act 2018.

3.5.14 The AO must be satisfied that there is a ‘pressing social need’ for the deployment and it is not reasonably viable to address this through less intrusive means, either because less intrusive methods have tried and failed or because there are reasonable grounds to believe that such tactics are unlikely to be effective.

3.5.15 Necessary on at least one of the following grounds:

- Necessary for Essex Police’s lawful policing purposes for reasons of substantial public interest; and / or
- Necessary for the administration of justice and / or
- Necessary for the safeguarding of children; and / or individuals at risk; and
- Necessary notwithstanding any expectation people may have pursuant to their article 8 human rights regarding the respect of private and family life, as well as other human rights considered by the AO; and
- Articulate that the AO has given due regard to the safeguards proposed for the deployment and the safeguards contained within the Essex Police LFR suite of documents. And, having given due regard to such safeguards considers that the deployment is a proportionate use of policing power when considering the use, and balancing them in the context of considerations relating to the Human Rights Act 1998, the Data Protection Act 2018 and UK GDPR; and
- Outline that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the watchlist complies with the Essex Police LFR suite of documents, including the legality, necessity, and proportionality criteria; and
- Articulate any authority to include additional categories of persons to the watchlist, including the legality, necessity, and proportionality criteria, in addition to those included to meet the purpose of the deployment; and
- Direct that all officers and / staff engaged in the deployment must have received LFR training as per the Essex Police LFR documents (unless they have received such comparable training as delivered by another UK Police Force)

3.5.16 Articulate that the AO considers the benefits of the deployment are proportionate to the impact on the public’s human rights and rights relating to equality.

3.5.17 Articulate that the AO is satisfied that the control measures in the data protection impact assessment, community impact assessment and equality impact assessment have been reviewed and that the AO considers them to be appropriate mitigants for the deployment.

3.5.18 Articulate what the AO’s minimum threshold setting to be utilised during the deployment. Ordinarily this setting will be equal to or above the value where no FRT

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

System bias is detected. The Threshold value may be lowered based on the intelligence case with a full rationale detailed in the EP LFR Application / Written Authority Document.

3.5.19 In cases where there is an urgent need to deploy LFR and an Authorising Officer not below the rank of Superintendent is not available then an Officer not below the rank of Inspector may authorise the deployment provided they are satisfied the request is urgent.

3.5.20 The officer not below the rank of Inspector authorising the deployment must inform an officer not below the rank of Superintendent of the authority as soon as practicable.

3.5.21 The Superintendent is then to authorise the continued deployment, make changes to the authority as they deem necessary or order its immediate cessation.

3.5.22 Should a further law enforcement purpose be identified after the AO has issued their authority for an LFR Deployment, processing in respect of the law enforcement purpose is not permissible unless the AO grants a further authority for it. Such authority would consider the lawfulness, strict necessity, and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.

3.6 Date, Time, Location and Duration of Deployment

3.6.1 The AO should define the date, time, location, and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment. The authority will cease and be officially cancelled at the time and date outlined on the application by the AO. The deployment cannot continue past this time without prior agreement from the AO either in writing or verbally if deemed necessary.

3.6.2 The applicant and AO will consider the following when determining the date, time, location, and duration: The intelligence case, policing purpose to include a person on a Watchlist, Community Impact Assessment and the environmental factors relevant to a potential Deployment.

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

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

- Policing information or intelligence about a proposed Deployment location including if there is an increased public safety risk and/or need to provide public reassurance at a Deployment location; and

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- The ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so.

3.7 When reviewing a potential Deployment location, AOs must also consider those who are likely to pass the LFR System and:

- **The reasonable expectations of privacy the general public may have as a whole at that location:**
- some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy Chelmsford town centre thoroughfare being typically different to a quiet suburban park or backstreet; and
- the number of cameras used by the LFR System should also be considered in this context to ensure the size and scale of the Deployment enables those on a Watchlist to be effectively located without disproportionately processing biometric data; *and*

3.8 If a proposed Deployment location attracts particular concerns by reference to those expected to be at a particular location:

- Hospitals, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), care homes and persons who may be attending a nearby assembly or demonstration are examples where those that attend them may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area.

3.9 Where it is practicable to identify a person of being responsible for a proposed Deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate.

3.10 Where privacy or other human rights considerations are identified in relation to a particular Deployment, the AO needs to consider the necessity to Deploy LFR to that particular location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is *necessary* (with the processing of data at that site being *strictly necessary*), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR System against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.

3.11 The public should be notified of LFR Deployments in advance using force websites and other appropriate communication channels (including social media).

3.12 Measures should also be taken during the Deployment to ensure 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. In addition to the use of uniformed

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

officers and marked vehicle(s), other steps for applicants to consider in the context of their proposed deployment location include the use of signage placed in advance (outside) of the Zone of Recognition and/or the provision of information leaflets. In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any deployment is overt, the objectives for the deployment and its use as a policing tactic will also be relevant if the policing need to deploy is to be realised. For example, unduly extensive signage may undermine the effectiveness of a deployment seeking to locate persistently outstanding offenders. By comparison a deployment seeking to protect a site or particular event may merit multiple levels of signs and the proactive distribution of leaflets to deter those with malicious intent.

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

3.14 Any member of the public who is engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. Any person who requires further information relating to LFR should be provided with contact information for the EP LFR operational team by e-mail to facial.recognition@essex.police.uk. **Watchlist Generation and Criteria for Watchlist Inclusion**

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

- Safeguards relevant to all Watchlists – Beginning at Section 3.5 - including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics.
- Who may be added to a Watchlist – Beginning at Section 3.6.1 - including in relation to police-originated, and non-police originated imagery.

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

Requirement	Rationale for the requirement
Intelligence: Watchlists must be driven by a policing need and based on the intelligence case The intelligence case must be current and reviewed before each Deployment.	This intelligence-driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR Deployment
Images sources: Watchlists must only contain images lawfully held by police with consideration also being given as to:	This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- the legal basis under which the image has been acquired; and - the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.	intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance. Additionally, policing has a responsibility to avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: - is of a person intended for inclusion on a given Watchlist; and; - is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator); LFR software settings have been reviewed and amended so that the minimum accepted face size of enrolment of pictures is now 100 pixels. The software will reject any image that does not reach this threshold.	This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that person should they pass the LFR System. This requirement and the prescribed False Alert Rate are also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The EP SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way. Three false positive alerts occurred in a short period of time during live deployments in Essex. Analysis of the FPs showed that this was down to the uploaded image quality rather than an error in the algorithm. The software has been assessed and settings changed to prevent any similar occurrence.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment.	This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours
Watchlist design: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated

3.16 In December 2020 the Surveillance Camera Commissioner (SCC) published his best practice guidance document '[Facing the Camera](#)'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist. Any controls, mitigations and processes identified by EP in this document reflect the EP LFR System's performance and EP's particular use-cases for LFR.

3.17 EP has confidence in the LFR System's performance, particularly in relation to gender, age and race. This has followed extensive academic and scientific studies of the algorithm to compliment local and pre-procurement testing by the provider. In 2025, Cambridge University and the National Physical Laboratory (NPL) conducted studies to test the algorithm for bias, aiming to ensure the Chief Constable meets legal obligations under the public sector equality duty.

3.18 EP recognises that *regardless* of performance considerations, it should take particular care when considering and publishing details relating to (i) age including the protection of children – particularly the very young, (ii) the disabled and (iii) those who have and/or are undertaking a gender reassignment. This is because:

- There may be different privacy expectations around the use of LFR and that these can be particularly relevant in relation to these people given their potential vulnerability.
- EP recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.

3.29 Documenting composition: EP provides that each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be:

- Aged under 18-years-old;
- Aged under 13-years-old;
- A person with a relevant disability;
- A person who has undertaken a gender reassignment and it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

Any use of an image of a child under the age of 13 would only be considered in high-risk cases.

3.20 The following outlines further, specific safeguards that apply to the composition of the watchlist:

	Age (U. 18)	Age (U.13)	Disability	Gender Reassignment
Circumstances				
	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 18-years-old	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old ⁷	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment
Safeguards				
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with EP LFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images		There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.		
Legal Advice		Specific advice must be sought from Legal Services and the EP LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		
Technical Advice	Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.			
	Consideration should be given to the likely crowd flow / occlusion risk where shorter	Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their		

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

	subjects may otherwise be blocked from the camera's line of sight.	decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.
--	--	---

3.21 Images that may be deemed appropriate for inclusion within an LFR watchlist include custody images of individuals and / or police originated images other than custody images of people who are:

- Wanted by the courts; and / or
- This term includes those with outstanding arrest warrants or who are otherwise required by the courts. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public at large.
- Suspected of having committed an offence or reasonably suspected to be about to commit an offence; and / or
- Subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment; and / or
- Missing persons categorised as 'Medium Risk' or 'High Risk'
- As defined by Missing Persons Authorised Professional Practice as posing a risk of likely serious harm to themselves or others.
- The reference images are sourced from Athena, Missing person database (COMPACT) and Images provided by public with consent.

3.22 A decision to include 'Medium Risk' or 'High Risk' missing person on a watchlist should be made based upon current missing people of these risk levels only who have an affiliation to that area through residency or intelligence linking them to that area or local policing division. All images from the missing person database are checked to ensure that they are of sufficient quality to prevent any false positive alerts. All images are pre-assessed by the software to ensure they are of the correct levels of pixelation.

3.23 At immediate risk of serious harm and not locatable or contactable by any less intrusive means.

3.24 Intelligence suggests the person poses an immediate risk of serious harm to another person. This refers to a person who has already been classified as High Risk through separate police assessment methods.

3.25 For a person to be included on the watchlist the Police must have a legal basis for action under a policing common law power.

3.26 The risk of harm will be informed by the intelligence case and/or the considerations set out in the applicable LFR form. This will need to inform the AO as to how the individual presents a risk of harm or why they are likely to suffer harm and:

- How using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

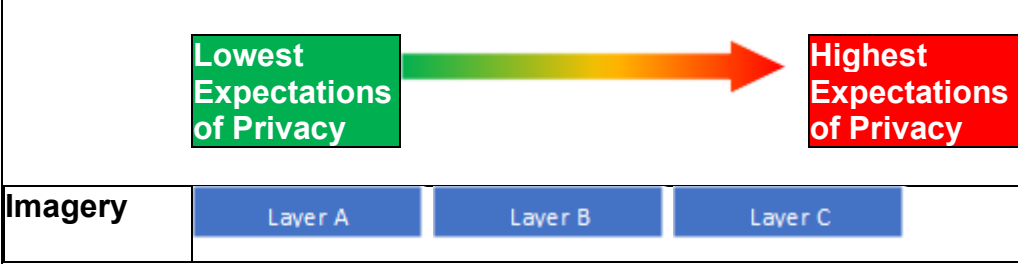
- Why the significance of the harm identified means it is **necessary** for the police to take action in order to manage the risk.

3.27 The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

- Any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
- The importance of locating the person or people sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;
- Whether the significance of the threat, harm and risk identified, which inclusion on the watchlist would address outweighs any expectations of privacy.

3.28 Where it is viable to do so without unduly impacting on the performance of the LFR System, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by EP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.

3.29 Non-police originated images are images which have not been taken by law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness.

Assessing Non-police originated sources of Watchlist imagery	
	
Image Layer	Outline
Non-police originated image– Layer A	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage; • circumstances where the police have obtained the image as a result of a lawful power of search or seizure;

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

	data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.
Non-police originated image– Layer B	Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject, including any imagery obtained pursuant to: - the Regulation of Investigatory Powers Act 2000; and - the Investigatory Powers Act 2016, Where the ability of relevant bodies to obtain such images is further supported and can be anticipated by reference to published Codes of Practice.
Non-police originated image– Layer C	Non-police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received. To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.

3.30 Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular which layer of intrusiveness the image is attributable to and the factors. The AO in these circumstances may wish to consult with the relevant Chief Officer as per 3.5.8.

3.31 The types of non-police originated images that may be deemed appropriate for inclusion within an LFR watchlist are of people:

- wanted by the courts; and/or
- suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
- subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; and/or) missing persons deemed increased risk; and/or
- presenting a risk of harm to themselves or others; and/or
- who are a victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation or is otherwise a close associate of

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

an individual and that individual themselves would fall within paragraphs (a) – (d).

- f) The reference images are sourced from Athena, Missing person database (COMPACT) and Images provided by public with consent. Images with consent will often be linked to missing people but could relate to crime such as a kidnap.

3.32 Essex Police LFR Documents

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

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

Note: *Any assessment listed above showing 'Review/Amend/Adopt' has already been created by the EP LFR team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each LFR operation.

3.33 Management of Risk and Resources Levels

3.34.1 Each Deployment should be risk assessed in line with EP procedure. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.

3.34.2 The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.

3.34.3 Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.

3.34.4 LFR System Engineers will be deployed to support LFR Deployments where required.

3.34.5 All EP officers and staff deployed on LFR Deployments must be compliant and in date with EP First Aid and where applicable officer safety (OST) training requirements. All EP officers and staff involved in an LFR Deployment must receive LFR training prior to being deployed.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

3.34.6 As part of the application process, the applicant should consult with the Operational Policing Command LFR team and or Covert Authority Bureau (CAB) to determine the appropriateness and viability of a deployment. This should be done before the application is submitted to the AO.

3.34 Cameras and Camera Placement

3.35.1 Cameras must be selected so that the image resolution, framerate, field-of-view and low-level light performance can provide images of sufficient quality for use in the facial recognition application. Current FR systems typically require a facial image with no less than 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED). The FR vendor should advise on specific requirements for their system.

3.35.2 Unless the environment is well controlled, cameras must be capable of operating at Wide Dynamic Range in order to generate high quality images under a variety of lighting conditions.

3.35.3 Cameras should ideally be positioned to capture faces as close as possible to the 'face-on' condition, similar to a passport image. This typically requires the cameras to be much lower than is normally the case for existing CCTV. Camera placement and angle should be further considered where those sought may be more likely to be occluded in a busy crowd in order to maximise the prospects of location.

3.35.4 Ideally the environment should be managed such that every face is evenly illuminated. Highly directional lighting, for example strong sunlight, should be avoided, which may require consideration of how the lighting will change throughout the day.

3.35.5 In general, the Zone of Recognition will be smaller than the field of view of the camera; for example, not all faces in the field of view may be in focus and not every face in the field of view will be imaged with the minimum necessary Inter-Eye Distance (IED).

3.35.6 A typical 2MP camera will provide sufficient resolution for LFR to work on a maximum of 3 to 4 people side by side. Therefore, consideration needs to be given to camera location and the physical environment. For example, looking for opportunities to funnel or restrict the movement of people within the Zone of Recognition. However, if the flow is reduced beyond a certain level, individuals may be grouped very close together, occluding or partly occluding the faces of people (people behind people).

3.35.7 Detection and processing of faces is an intensive task for a computer system. The supplier of LFR software should provide guidance on hardware requirements and the number of faces that can be simultaneously processed from within a single frame. If the system is set to process too many faces, this will potentially result in delays to the LFR system response. It may also result in missed Alerts due to 'dropped frames' where the software skips some of the video footage in an attempt to catch up.

3.35 LFR Operational Roles

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

LFR Command Team

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

- Gold Commander (Superintendent or above); There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their 'strategic intention' aligns with the Written Authority Document. Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold will also liaise as necessary with NPCC ranked officers. Gold can also perform the AO role.
- Silver Commander (Chief Inspector or above); There is only one Silver Commander for any LFR Deployment. Silver reports to Gold. Silver has tactical command of the Deployment and is responsible for tactical implementation. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having particular regard to the effectiveness of the safeguards in place whilst LFR is being used.
- Bronze Commander (Sergeant or above); Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with sufficient clarity and ensure that they are fully understood by all officers and staff involved in the Deployment.

3.36.2 Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative command team terminology or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

3.37 LFR Operator

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

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

3.37.3 The LFR Operator's log should include: -

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- The LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; and
- what decision was taken regarding whether to Engage a member of the public or not; and
- whether an Engagement was successfully undertaken, and the outcome of the Engagement.

3.38 LFR Engagement Officer

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

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

3.38.3 The LFR Operator may be supportive of an engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.

3.38.4 When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal. There is a four-stage process leading to an appropriate outcome.

STAGE 1 – LFR software alerts to a potential match on the watchlist. LFR operator will visually assess the two images and only notify an engagement officer if they believe the match is correct.

STAGE 2 – Engagement officer will approach the individual and confirm their identity via personal documentation or fingerprint device if appropriate.

STAGE 3 – Engagement officer will then assess and decide on the appropriate form of disposal.

STAGE 4 – If an arrest takes place, then the appropriate custody department and the officer in the case will be notified.

3.38.5 Whilst officers must exercise their own discretion when using their powers of arrest and detention, EP policy is that an LFR application-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

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

3.38.6 If an 'Engaged Individual' cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

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

3.38.8 Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so. If other lawful orders are in existence where there is a requirement to remove face coverings (i.e. Sec 60) then the silver commander will direct officers deployed accordingly in line with the legal direction. There are no common powers to require someone to remove a face covering outside specific legislation.

3.39 LFR System Engineers

3.39.1 LFR System Engineers have enhanced technical training for the Deployment of LFR (see EP LFR Policy Document for further information). LFR System Engineers are responsible for the set-up of the LFR equipment and the optimisation of the LFR application to maximise performance.

3.40 Public Engagement

3.40.1 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.

3.40.2 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

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.

3.40.3 Key stakeholders, including the PCC'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.

3.40.4 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 SOP; and
- c) literature is prepared for persons who may be engaged (to include information outlined within a privacy notice); and
- 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.

3.40.5 During deployments EP will ensure that:

- a) awareness raising measures are used in line with the EP LFR SOP 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.

3.40.6 After deployments EP 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

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- 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) engagement with representatives from the Information Commissioners Office will be ongoing.

3.40.7 Post-Deployment

- a) Following each LFR Deployment, the Silver Commander must ensure that a post Deployment evaluation is completed which is updated in the Deployment Record. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both qualitative and quantitative in nature.
- b) The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the Deployment and what opportunities exist to improve them for future use, and how learning will be shared.

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

- total number of individuals and the total number of images included in the Watchlist (there may be multiple images of some individuals); and
- total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR application was able to generate a Template from them); and
- total number of LFR application-generated Alerts; and
- total number of Alerts that do not result in an Engagement; and
- total number of Alerts where a decision was taken to Engage an individual; and
- total number of Alerts that are confirmed as true alert (the individual is who the LFR application suggests are); and
- total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and
- total number of correct Alerts that result in an Engagement that do not require any further police action; and
- outcome of each case where police action is instigated following an Alert; and
- number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome; and
- Threshold setting for the Deployment.
- OPC complete the alerts spreadsheet which includes full details of the individual including their age, sex and ethnicity. The outcome of the alert i.e. arrest and the disposal.

3.41 LFR Application Security

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

3.41.1 The LFR application includes a number of physical and technical security measures. These include: -

- Images are transferred onto the LFR application within Essex Police premises as it is not possible to share encrypted devices between technologies that are not compatible with the force ICT network and associated devices. Force ICT do, however, allow for authorised personnel to be added to a security group which allows for non-encrypted removable media to be used. This media will still be scanned by the force Checkpoint Endpoint security for any vulnerabilities and this will strictly prohibit access to any devices containing executable code, exe, com, dlls and such like.

3.41.2 The LFR application is a fully closed system with two layers of password protection to access the application; and

3.41.3 The LFR application is physically protected when in use and deployment data stored on the system is securely wiped following each Deployment; and

3.41.4 Role based access controls with limited user permissions are implemented on the LFR application; and

3.41.5 The LFR application can be connected to mobile devices using a private access point with three levels of protection: Specific IP addressing,

3.41.6 Password access to the access point, and password access to the mobile App.

3.41.7 The Dashboard and RESTful API are secured with SSL and TLS by default; and all connections are directed through HTTPS; and

3.41.8 A full audit is maintained of all users initiated actions undertaken during the course of a Deployment; and

3.41.9 technical issues with the LFR application are always dealt with by LFR System Engineers deployed on the operation.

3.42 Data Retention and Data Management

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

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

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

3.42.2 All personal data from the software and watchlists from each deployment is deleted as soon as practicable or any case within 24 hours other than details of those subject to a positive alert. If any data is retained for evaluation purposes this would be appropriately documented in line with Data Protection legislation. That data would only ever been retained for the period of assessment only.

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

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

3.42.4 To support compliance the LFR application has a full audit capability, and the LFR Operator and LFR Engagement Officer log is retained in line with MOPI retention periods.

3.42.5 The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether protected by encryption, must be reported immediately to the AO, Gold, and the EP Data Protection Officer.

3.43 Register of Deployments

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

- Name and rank of the AO and command team; and
- Date, time, duration, and locality of Deployment; and
- Watchlist composition statistics (not including any personal data); and
- The number of Alerts and the various statistics relating to these; and
- Number of Engagements and their results.

3.43.2 EP will make information relating to LFR Deployments available to the public in accordance with the EP LFR Documents.

3.44 Contact Information

3.44.1 The Essex Police LFR team can be contacted on facial.recognition@essex.police.uk

3.45 Governance & Oversight

3.45.1 The following stipulations are accepted by Essex Police:

- The overall benefits to the public must be balanced with public confidence of our use of LFR.
- It can be evidenced that the technology itself will not result in unacceptable gender or racial accuracy variance into policing operations.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- Each deployment must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific policing purpose.
- 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.
- Essex Police 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.
- A quarterly review of the positive alerts will take place analysing the performance of the deployments and the analysis of the special characteristics of the individuals subject to alert i.e. a breakdown of age, gender, ethnicity together with arrest and disposal outcomes.

3.45.2 Governance and oversight of the use of the technology is approached in the three stages below:

- Pre-deployment
- Operational deployment
- Post-deployment

3.45.3 Pre-deployment:

- Authority to deploy LFR is an operational one, where an Essex Police 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.
- 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.
- Prior to AO authorisation and the deployment of LFR in public spaces, several documents must be completed and an Essex Police officer of Chief Officer rank¹ (or police staff equivalent) must be made aware by the AO. Whilst the Chief Officer does not provide authority for LFR deployment, consultation at this level exists to expose the proposed deployment to an elevated level of strategic thinking in line with the circumstances described at 3.5.8, whereby issues are considered as much as possible. This affords the Chief Officer the opportunity to scrutinise the deployment and to ask the AO to consider what mitigation is required to address concerns at hand.
- Several specific Essex Police documents and records need to be completed in support of each deployment. These are set out below:

¹ NPCC – 'NPCC rank' denotes an officer holding the rank of ACC or above.

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

Essex Police 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.
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 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.

3.46 Several other specific Essex Police documents pertaining to each Essex Police LFR deployment have been completed centrally. These are set out below:

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

Essex Police LFR Documents and Records	
Essex Police Data Processing – Appropriate Policy Documents	Essex Police policy on the processing of data pursuant to the Data Protection Act 2018 and UK General Data Protection Regulation relating to LFR.
Essex Police Legal Mandate	Outlines the legal considerations to be addressed to use LFR.
Essex Police	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.

3.47 Oversight bodies and Regulatory Framework

3.47.1 Within EP, the senior internal oversight body for LFR is the FR Strategic Governance Board. In addition, The EP PFCCs office also provide an external oversight and scrutiny perspective.

3.47.2 EP LFR Legal Mandate sets out the legal framework for EP use of LFR technology, whilst EP LFR Policy Document and this EP LFR procedure document support implementation.

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

3.47.4 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 Surveillance Camera Commissioner, the Biometric Commissioner and the Essex Data Ethics Committee. More detail on these roles:

- Surveillance Camera Commissioner (SCC); The role of the Surveillance Camera Commissioner is to encourage compliance with the surveillance camera code of practice, review how the code is working, provide advice to ministers on whether the code required amendment. Any EP LFR system will need to comply with this Code and the twelve guiding principles. This guidance document seeks to apply those principles. See www.gov.uk/government/organisations/surveillance-camera-commissioner
- Biometrics Commissioner (BC); The Commissioner is independent of Government and aims to keep the police use and retention of biometric data under review. The Commissioner makes decisions on applications made by the police to retain DNA profiles and fingerprints, and reviews national security determinations that are made or renewed by the Police in connection with the

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

retention of DNA profiles and fingerprints. The Commissioner also reports to the Home Secretary about the carrying out of their functions. See:

www.gov.uk/government/organisations/biometrics-commissioner

- [Information Commissioner's Office \(ICO\)](http://www.gov.uk/government/organisations/information-commissioners-office); 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 and should be shared with the ICO. See www.gov.uk/government/organisations/information-commissioners-office
- [The Essex Data Ethics Committee](#); [The Data Ethics Committee](#) are an independent source of advice. Their terms of reference include the provision of advice and independent oversight of Essex Police on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework.

4.0 Equality Impact Assessment

EIA – February 2026

5.0 Risk Assessment

- 5.1 Each Deployment should be risk assessed in line with EP procedure. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.
- 5.2 The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.
- 5.3 Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.
- 5.4 LFR System Engineers will be deployed to support LFR Deployments where required.
- 5.5 All EP officers and staff deployed on LFR Deployments must be compliant and in date with EP First Aid and where applicable officer safety (OST) training requirements. All EP officers and staff involved in an LFR Deployment must receive LFR training prior to being deployed.

6.0 Consultation

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

OFFICIAL – POLICE PERSONNEL ONLY

Page 27 of 29

Version 1, September 2024

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

- 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
- Legal

7.0 Monitoring and Review

The author will carry out intermittent reviews for legislation, any process changes and will carry out yearly reviews of the whole document.

8.0 Governing Force policy.

Related Force policies or related procedures

8.1 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](#).

8.2 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/>.

9.0 Other source documents, e.g., legislation, Authorised Professional Practice (APP), Force forms, partnership agreements, (if applicable)

PROCEDURE – Live Facial Recognition

Number: D 2701

Last Updated: 8th March 2026

Version 1 – September 2024

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

- Information Management APP; <https://www.college.police.uk/app/information-management>
- National Decision Model; [National decision model | College of Policing](#)
- National Intelligence Management; [Intelligence management | College of Policing](#)
- [College of Policing Code of Ethics](#)
- Home Office Biometric Strategy – Published June 2018; www.gov.uk/government/publications/home-office-biometrics-strategy
- [High Court Ruling – R \(on the application of Edward Bridges\) v The Chief Constable of South Wales \[2019\] EWHC 2341 \(Admin\):](#)

Procedure Author: D/SUPT Stephen JENNINGS – SCD

Procedure Owner: ACC Simon WILSON – ACC SCD

Cancellations: N/A