

Policy



Overt Deployment of Live Facial Recognition Technology

DCP-P-097

Version 1.0

Effective date 13/07/2026

Version date 13/07/2026

Review date 13/07/2028

Host Force Devon & Cornwall

Host Policy Unit Devon & Cornwall

Policy Owner Intelligence Directorate

Policy Author Chief Inspector, Intelligence Directorate

Associated procedures

Live Facial Recognition Standard Operating Procedure

1. Policy summary

This policy will detail the requirements for the deployment of Live Facial Recognition (LFR) technology within Devon & Cornwall Police (DCP).

This policy aims to:

- a) Provide DCP officers, staff, volunteers and contractors (to be referred to as officers and staff throughout this policy) as well as members of the public with information about DCP's present strategic, operational and technology objectives for the overt use of LFR, such that it enables DCP to achieve their law enforcement purposes and is compliant with key recommendations (the objectives); and
- b) Provide DCP officers and staff with guidance on the deployment of overt LFR technology by DCP in spaces accessible to the public to meet DCP's objectives for LFR; and

- c) Establish the governance structure for the deployment of LFR, ensuring that DCP use of LFR is appropriately governed, ethical and legally compliant; and
- d) 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.

2. Purpose, standards and legal basis

2.1 What is LFR technology and why will we use it

LFR works by analysing key facial features to generate a mathematical representation of them, the Biometric Template. This representation is then compared against known faces in a database to identify Possible Matches against persons of interest to law enforcement agencies. Where the LFR system identifies a Possible Match, the LFR system flags an alert to a trained member of DCP officers and staff (or trained personnel from a force that is supporting with the deployment) who then decides whether any further action is required.

In this way, the LFR system works to assist DCP officers and staff to make identifications rather than acting as an autonomous machine-based process devoid of user input.

DCP believe that LFR is a valuable precision policing tool that is less intrusive than alternatives and will help DCP keep the public safe, meet common law policing duties, including reducing violence and the risk of harm, the prevention and detection of crime, the preservation of order, apprehend and prosecute offenders and maintain public confidence.

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. DCP are 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 (such as race, ethnicity and other bias) and the instances of false-reporting relating to the accuracy of LFR (particularly in the context of early deployments by other forces), the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.

It is therefore incumbent on DCP to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR.

2.2 LFR technology in scope of this policy

Currently, the only circumstances in which DCP will deploy LFR is listed below. This may change as DCP's approach to LFR evolves, in which case this policy and related documentation would be reviewed and updated accordingly.

- a) For the purpose of locating persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison. This will only include those persons who have not been located despite previous proportionate enquiries to do so.
- b) For the purpose of locating individuals who are designated as a current high risk missing person.
- c) Suspects wanted for high risk offences including, but not limited to homicide, rape, serious violence, serious sexual offences and robbery.
- d) Suspects wanted for offences where a local community priority is identified which justifies the inclusion.
- e) To identify persons with police or court imposed conditions or orders that may be breached if identified as being at the deployment location.
- f) Significant public events with risk of public order offences.
- g) Where a significant and imminent threat has been identified and LFR can be utilised to identify suspect(s).

The inclusion of any category will be determined for each operation, commensurate with the intelligence case and identified threat and risk posed.

2.3 Facial recognition technology not in scope of this policy

There are other forms of facial recognition technology that are not subject of this policy. This includes retrospective facial recognition, which relates to non-real time searching of images against a database. Also not in scope is operator initiated facial recognition 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' environment.

In summary, this policy does not extend to:

- a) Manually instigated facial recognition for retrospective searching of video / still images; or
- b) Human initiated facial search submitted from a mobile device in near real-time; or
- c) The covert deployment and use of LFR technology; or
- d) Any DCP use of third-party LFR systems used for a commercial purpose or data sharing for the purpose of facilitating the use of a commercial system. In such instances additional privacy considerations would be required (e.g. additional Information Sharing Agreements and audit requirements), which are beyond the scope of this policy; or

- e) The legal framework that is applicable to DCP's use of LFR – this is separately detailed within the Legal Mandate document.

2.4 Legal basis

LFR deployments and any information collated or created from those deployments will be managed accordingly in line with, but not limited to, the following guidance and legislation:

- The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR)
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Freedom of Information Act 2000
- Equality Act 2010
- The College of Policing Authorised Professional Practice on LFR
- Information Commissioner's Office (ICO): Facial recognition technology and surveillance
- ICO: The use of LFR technology in public places
- Home Office Biometric Strategy
- Section 60AA of the Criminal Justice and Public Order Act 1994
- Code of Practice for Police Information and Records Management (PIRM, formerly known as Management of Police Information/MOPI)
- Code D of the Police & Criminal Evidence Act 1984
- NPCC Digital imaging and multimedia procedure v3.0
- International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC)
- Criminal Procedures and Investigations Act 1996
- British Standards Institute
- British Standards Institute: guide to safe and ethical use of facial recognition tools launched
- British Standards Institute: facial recognition technology – ethical use and deployment in video surveillance-based systems code of practice BS9347:2024
- Biometrics and Surveillance Camera Commissioner – code of practice and the 12 guiding principles
- Authorised Professional Practice
- National Decision Model
- Force Purpose and Objectives
- Equality and diversity matters including the Public Sector Equality Duty and Code of Ethics (ethical policing principles and guidance for ethical and professional behaviour in policing)

2.5 Oversight bodies and regulatory framework

The Office of the Police and Crime Commissioner (OPCC) for DCP provides an external oversight and scrutiny perspective.

Nationally, the ‘National Police Chiefs Council (NPCC) Facial Recognition Technology Board’ provides oversight for the operational uses of facial recognition within UK law enforcement. DCP will make contact with the Board to ensure wider understanding and support for national objectives and priorities.

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 ICO, and the Biometrics and Surveillance Camera Commissioner. The role of the Biometrics and 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 requires amendment, and to keep the police use and retention of biometric data under review, including making decisions on applications made by the police to retain DNA profiles and fingerprints, and reviewing national security determinations that are made or renewed by the police in connection with the retention of DNA profiles and fingerprints. The Commissioner also reports to the Home Secretary about the carrying out of their functions.

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 of the Data Protection Act 2018 and/or Article 35-36 UK GDPR should be shared with the ICO if, after assessment, the use of LFR poses any high privacy / compliance risks that cannot be mitigated.

2.6 Additional documents to support deployment(s) of LFR

A number of documents have been created by DCP to enhance this policy, and these include, but are not limited to:

- a) LFR Standard Operating Procedure
- b) LFR Data Protection Impact Assessment
- c) LFR Legal Mandate
- d) LFR Appropriate Policy Document
- e) LFR Equality Impact Assessment
- f) Surveillance Camera Code Self-Assessment
- g) LFR Privacy Notice
- h) The LFR training documents and guides used by DCP or other officers supporting them with LFR deployments (‘the LFR Documentation’).

In addition, in relation to any deployment(s), there will be a LFR Application, LFR Authorisation, a Watchlist and the LFR Deployment Records.

2.7 Terminology and acronyms

Refer to Appendix A for terminology and Appendix B for acronyms used by DCP in all LFR documents.

3. Roles & responsibilities

Administrator

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

Authorising Officer (AO)

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

Gold Commander

An 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.

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.

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.

LFR System Manager

DCP retains overall accountability and responsibility for decisions where technical capability is affected, this includes performance, maintenance, fault resolution as well as responsibility for the vehicle and associated deployment infrastructure.

Silver Commander

An 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.

4. Policy information

4.1 Objectives

LFR deployments must be run under a written Authority Document that complies with the following objectives.

4.1.1 Strategic objectives

DCP will:

- a) Use overt LFR technology in a responsible way and in accordance with policy in order to locate offenders in compliance with common law policing powers. This includes targeting those wanted by the courts under an arrest warrant, sought for recall to prison, suspected of relevant criminal offences and high risk missing people.
- b) Strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep Devon and Cornwall safe.
- c) Build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns, legitimacy concerns and maximising transparency.
- d) 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.
- e) 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 courts, the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and LFR documents.
- f) Transparently identify, manage, and mitigate reputational and organisational risk to DCP.
- g) Be recognised as a progressive, responsible, and ethical organisation.

4.1.2 Operational objectives

DCP will:

- a) 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;
- b) Engage with and provide reassurance to communities, listening and responding to concerns; and
- c) Continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

4.1.3 Technological objectives

DCP will:

- a) Ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and

- b) Provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic; and
- c) Look to technological improvements whilst keeping the LFR Standard Operating Procedure under review. Where appropriate we will trial 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. Any trial will have relevant documentation and considerations completed prior to commencement.

4.1.4 Consultation and engagement objectives

Following consultation within DCP and the communities they serve, the following stipulations have been proposed and accepted by DCP.

- a) The overall benefits to the public must be balanced with public confidence of our use of LFR;
- b) The Independent National Physical Laboratory testing demonstrates no significant statistical bias in the matching algorithm, in relation to gender, race or age when set to 0.6 or higher. DCP will deploy LFR with a configured threshold of 0.64;
- c) Each deployment must be appropriately assessed and authorised, demonstrating both necessity and proportionality 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) DCP 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 Biometrics Strategy's requirement for transparency and the Statutory Surveillance Camera and Biometric Commissioner's code of practice, as well as guidance issued by the Information Commissioner and the courts. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime. This will include Independent Advisory Groups, the Ethics Committee and Policing Governance Boards/Panels.

4.2 Overview of effective LFR deployment

4.2.1 End-to-end process

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

- a) Mechanism in place to direct persons wishing to access more information about DCP's use of LFR, exercise their data protection rights or complain;
- b) LFR law enforcement purpose identified, safeguards considered, deployment authorised, and Watchlists selected in the 24 hours prior to deployment time;
- c) Biometric templates extracted from images of individuals included in Watchlist;
- d) Notification of deployment and signage deployed;
- e) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist;
- f) If a possible match is found in a Watchlist, the LFR system 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;
- g) The LFR Operator / LFR Engagement Officer will consider the alert, (including the image comparison and confidence score), 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;
- h) Cancellation of authority for the LFR deployment and post-deployment evaluation.

The LFR Standard Operating Procedure provides a greater level of detail about the processes involved in the deployment of LFR by DCP.

4.2.2 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.

The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, 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.

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

This will be discharged by:

- a) Having printed LFR information leaflets at deployments for DCP Engagement Officers to provide to any persons they have spoken to as a result of a confirmed LFR match, and any persons in and around the recognition zone;
- b) QR codes and links on LFR leaflets and posters directing individuals to additional LFR information on DCP's publicly accessible digital platforms such as websites;
- c) Publication of the LFR documents, results of previous LFR deployments and Frequently Asked Questions on the DCP Force website (redacted as necessary);
- d) Details of deployments will be published on the DCP Force website and social media channels ahead of deployments (usually 7 days prior to deployment);
- e) DCP Engagement Officers will answer questions asked by individuals around the deployment area and be able to direct individuals to further information;
- f) Providing a mechanism for individuals to contact DCP for further information or complain.

5. Stages of deployment

Governance and oversight of the use of LFR is approached in three stages:

- a) Pre-deployment;
- b) Operational deployment;
- c) Post-deployment.

5.1 Pre-deployment

5.1.1 Pre-deployment - introduction

Authority to deploy LFR is an operational one, where DCP AO rank is set at Superintendent.

Prior to AO authorisation and the deployment of LFR in public spaces, several documents must be completed and a DCP officer of NPCC rank (or police staff equivalent) must be engaged by the AO. Whilst the NPCC do not provide authority for LFR deployment, consultation at this level exists to expose the proposed

deployment to an elevated level of strategic thinking, whereby issues are taken into account as much as possible. This affords the NPCC the opportunity to scrutinise the deployment and to ask the AO to consider what mitigation is required to address concerns at hand.

The DCP Ethics Committee is an independent source of advice. The terms of reference include the provision of advice and independent oversight of DCP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework. The Ethics Committee has been consulted prior to the first use of LFR in DCP and will continue to be engaged as required.

Several specific DCP documents and records must be completed in support of each deployment. These are set out below:

DCP LFR deployment - documents and records	
LFR Application	Sets out the details of a proposed deployment including location, dates/times, impact on the community, 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, strict 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 PIRM 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 authorising 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 a LFR deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.

Several other specific documents pertaining to each DCP deployment have been completed centrally and referenced here.

5.1.2 Pre-deployment - LFR safeguards

DCP will adopt the following safeguards when using LFR:

- Each deployment must be carefully designed and have clear, documented objectives.
- The Watchlist for any deployment will be restricted to individuals described above, linked to the purpose of the deployment and where there is considered to be a likelihood of individuals from those Watchlists being in the vicinity of that deployment.
- The AO must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality.
- Whilst considering proportionality, for each deployment the AO should address how the public benefits from the use of LFR and how this compensates for any impact on the human rights of the public.
- Additional safeguards include: transparency, training, consultation, data retention and destruction, a threshold of seriousness and the quality and source of input images.
- The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the deployment are appropriately trained, briefed, and accountable.

- That equipment will be used correctly, and that those involved in the deployment mitigate against inappropriate responses to LFR system alerts.
- 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 system have been considered, and what safeguards are in place to protect them.
- Will deliver transparency by responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people from DCP communities.

5.1.3 Pre-deployment – public engagement

Key stakeholders and the OPCC will be notified in advance of any deployments and given as much information as they require to understand where, when and why there is a need for an LFR deployment. This engagement will usually take place 7 days in advance of the deployment, however this may be shorter if urgent operational need arises and can be justified. Whilst the deployment of LFR is an operational matter, the support of the OPCC is crucial to its success and legitimacy.

Operational briefings delivered to officers and stakeholders prior to deployments should promote openness with the public and transparency about the use of LFR, and officers are 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.

In advance of deployments DCP will ensure that:

- a) LFR deployments are notified to the public (usually 7 days prior to the deployment) using the DCP website and other appropriate communication channels (including social media) which should be underpinned by a press and media strategy giving advance notice of deployments; and
- b) LFR awareness raising measures (e.g. signs and leaflets) are prepared to support LFR deployment in line with LFR Standard Operating Procedure; and
- c) LFR 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, limits and the effects the use of LFR could have on communities and public trust. 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 DCP 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.

5.1.4 Pre-deployment – Watchlist image quality

The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. Any images of insufficient quality will be technically prevented from extracting a biometric template and being uploaded into the LFR system. Whilst it will usually be the case that images populating the Watchlist will have been previously collected in police custody, on a person's arrest, and are lawfully held by the police (and therefore likely to be relatively recent). On occasion, it may be necessary to populate the Watchlist with images that are not police held custody images, for example images of high risk missing persons provided by their families. In such cases, any additions whether pre or during deployment will be authorised by the AO and any anticipated use of non-police sourced images will be highlighted in the LFR Application. Code D of the Police & Criminal Evidence Act 1984 allows the images to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions. The best images are those that follow a custody or passport style image that conforms to the NPCC Digital imaging and multimedia procedure v3.0.

5.1.5 Pre-deployment - compiling the Watchlist

The Legal Mandate provides commentary on the legal considerations relevant to compiling a Watchlist in a lawful way. This means that DCP ensures the Watchlist images held are lawful, 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 a deployment.

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. The LFR Standard Operating Procedure provides practical guidance on how to follow the LFR documents, including the Legal Mandate.

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.

LFR helps locate those on a Watchlist by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist of Candidate Images of people who are wanted. Watchlist composition is normally restricted to individuals considered likely 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. The likelihood of an individual being in proximity of an LFR deployment 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 DCP they might be found. Factors for consideration in this respect include:

- a) Severity of offence in question; this will often be relevant to the risk posed and / or the level of urgency associated with locating and arresting an individual as well as the anticipated impact on their conduct. 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, such as previous offending in the area (generally or specifically by the individual), local transport links and other amenities, may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the Watchlist;
- d) Offender; offenders suspected to reside in or frequent the relevant deployment location or whether no known residential address is available for the offender.

Ensuring the quality of images included on the watchlist does not reduce the efficacy and accuracy of facial matching is the responsibility of the LFR Silver Commander to ensure the following safeguards are implemented per deployment:

- a) The most up to date police sourced or non-police sourced images of a person who meets the criteria for inclusion on the Watchlist will be extracted for LFR use.
- b) By using image 'ingestion settings' (such as distance between eyes, facial quality and facial reliability, face tilt) that have proven to be reliable the LFR system has a technical safety net which exists to prevent images of poor quality from being uploaded onto the LFR system.
- c) Reviewing the proposed Watchlist images prior to uploading, with particular attention paid to non-police sourced images (e.g. for high risk missing persons), in combination with the briefing of LFR Operators and Engagement Officers enabling them to pay due regard to image quality and age when considering facial matching alerts.

5.1.6 Pre-deployment - governing the Watchlist

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 the data protection principles.

The 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.

If the LFR system cannot be connected to the Force network, the Watchlist will be downloaded to an encrypted data stick. 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. When the deployment has finalised the data stick will be securely deleted or destroyed once the required retention period has passed.

5.1.7 Pre-deployment - design guidelines for LFR

An international standard (ISO IEC 30137-1: Use of biometrics with video surveillance systems, Part 1: System design and specification) was published in May 2019. Edition 2 published in 2024, ISO IEC 30137-1:2024, provides additional detail covering technical aspects of specifying and implementing a facial recognition system for use with video cameras, including camera selection and placement, adjustment of detection and matching Thresholds, Watchlist management, and the role of the LFR Operator. It is strongly recommended that forces considering the use of LFR use the guidance to supplement the technical overview provided here. DCP will do this and, where they use the assets of other forces, ensure that they have done this.

DCP LFR processes and associated guidance have been developed to provide a reliable means of locating individuals using LFR with high-definition CCTV cameras (2MP and above). For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the LFR Operator, and associated policing resources on the ground.

A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this guidance.

Directly relevant components include:

- a) The cameras, including cabling, and their placement; and
- b) The environment in which the cameras operate; and
- c) The database of reference images and associated meta data, often referred to as the Watchlist; and
- d) The facial recognition software that detects faces in the footage, converts the facial images into templates, compares these against the Watchlist and provides information on the results of the comparison (generally in the form of an alert or a numerical score) to an LFR Operator; and

- e) The LFR Operator and LFR Engagement Officer who assess alerts and determine the appropriate course of action; and
- f) Having sufficient officer resource to support the deployment.

5.1.8 Pre-deployment - cameras and camera placement

Cameras must be selected so the image resolution, frame rate, field-of-view and low-level light performance can provide images of sufficient quality for use in the facial recognition application. Currently systems typically require a facial image with between 20 and 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED). The facial recognition vendor should advise on specific requirements for their system.

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.

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.

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.

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 or IED.

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). This will only be done using existing physical architecture and objects which are not placed to facilitate the LFR deployment.

Any deployment of LFR cameras will only take place where there is a likelihood of locating persons included within the Watchlist. A range of factors will be relevant to this assessment and these include the nature of the site itself, available intelligence including previous criminality and the policing need to be at the site (including for the public's protection, suppressing crime hotspots, and getting ahead of crime trends), Watchlist composition and the perceived attractiveness of the location to wanted

individuals. Further considerations as to the appropriate location include the implications for human rights and the risks arising from collateral intrusion.

5.1.9 Pre-deployment - deployment location

The selection of a location for a deployment will be based on a number of countervailing factors including:

- a) Intelligence regarding the previous criminality conducted in the relevant area, i.e. status as a crime 'hotspot' and/or by individuals on the Watchlist;
- b) Watchlist composition and nature of threat;
- c) Nature of location, i.e. residential, commercial etc.;
- d) Local amenities, such as transport links, retail and leisure offering;
- e) Local sensitivities, such as schools, medical facilities, religious or other cultural organisations;
- f) Any anticipated demonstrations or other assemblies; and/or
- g) Availability of alternative routes.

The weight to be accorded to each of these factors will depend on and vary between each specific deployment.

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 DCP in discharging their operational duties. The decision to deploy LFR will 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 LFR documents with regard to Authorised Professional Practice.

5.2 Operational deployment

5.2.1 Operational deployment - introduction

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

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 that:

- a) The use of the LFR remains strictly necessary and proportionate for the policing purposes identified in the Written Authority Document; and
- b) The safeguards identified in the written approval remain effective; and

- c) The level of officer support committed to the deployment is enabling alerts to be responded to effectively; and
- d) The Subject, System and Environmental Factors are such that the use of the LFR system remains effective for realising the policing purpose identified in the written approval.

Circumstances may arise that mean 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 Standard Operating Procedure.

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 system performance and the engagements undertaken.

5.2.2 Operational deployment – public engagement

During deployments ensure that:

- a) Awareness raising measures are used in line with the LFR Standard Operating Procedure to ensure that policing presence is overt so 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 the DCP website are available to hand out to the public on request delivering important key messages aimed at promoting trust and confidence through improved understanding, along with redress routes and data subject rights; and
- c) Information is offered to persons engaged by officers in accordance with the policy.

Dependent on the circumstances of an LFR deployment, further public engagement approaches may need to be considered.

5.3 Post-deployment

5.3.1 Post deployment - introduction

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.

Any complaint received will be managed and allocated by the Professional Standards Department.

Each deployment should be subject of an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO (this may be the same person as the Silver Commander) to ensure that appropriate senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

The outcomes of LFR deployments are subject to evaluation, which in turn should feed into oversight and scrutiny processes.

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

- a) Where the LFR system does not generate an alert, that person's biometric data from the live LFR CCTV feed is immediately automatically deleted;
- b) Where the LFR system does generate an alert, that person's biometric data from the live LFR CCTV feed is deleted within 24 hours following the conclusion of the deployment; and
- c) The data held on an encrypted USB memory stick used to import the Watchlist onto the LFR system is deleted within 24 hours following the conclusion of the deployment.

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

- a) Due to its relevance in a criminal investigation and is held in accordance with the Data Protection Act 2018, UK GDPR (where applicable), PIRM and the Criminal Procedures and Investigations Act 1996; and /or
- b) In accordance with DCP's complaints / conduct investigation policies or other legal obligations.

5.3.2 Post deployment – public engagement

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 the DCP website within 31 days. Care must be taken to ensure that no personal data is published;
- b) External engagement is considered in discussion with DCP 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.

5.3.3 Post deployment - key performance metrics

DCP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool, utilising reports such as the National Physical Laboratory facial recognition technology in law enforcement, and equitability study final report, March 2023.

This section covers some of the key performance metrics that should be gathered when deploying LFR. It outlines the minimum requirements and so additional metrics or indicators may well be relevant and suitable for collation and analysis. The key metrics that determine the ‘accuracy’ of an LFR system are:

- **True Recognition Rate**

The number of times when individuals on a Watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times when these individuals passed through the zone of recognition (regardless of whether an alert is generated).

This metric can only be generated by ‘seeding’ known subjects (for example police officers or staff) into a Blue Watchlist and measuring the number of times those subjects are present in the Zone of Recognition against the number of alerts generated. Users of facial recognition systems (and vendors) must not focus so closely on maximising this metric that they increase the False Alert Rate to inappropriate levels.

An example of the True Recognition Rate can be found within Appendix A.

- **False Alert Rate**

There are two types of False Alert Rate measurements. The first is the System False Alert Rate, 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 False Alert Rate, which is calculated in the same way, but is measured after the LFR Operator has reviewed the output from the LFR system and dismissed LFR system alerts assessed by the LFR Operator as false.

All of the True Recognition Rate and False Alert Rate metrics should be recorded and reported. Operational experience of other forces to date suggests that in most scenarios the False Alert Rate should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the False Alert Rate 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.

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 True Recognition Rate and False Alert Rate. The threshold needs to be set with care to maximise the probability of returning correct Possible Matches, whilst minimising the number of False Alerts. DCP will deploy LFR with a configured threshold of 0.64 demonstrating a low tolerance for false matches at a level which also minimises the risk of bias or discrimination. The accepted tolerance for false matches, is a False Alert Rate of 1:1000 which seeks to balance the countervailing interests in a proportionate way but in practice it is noted that at the configuration threshold of 0.64, the False Positive Identification Rate/False Alert Rate performed significantly better both in scientific testing by the National Physical Laboratory and having regard to the operational experience of South Wales Police. In addition, the number of false alerts as a proportion of the total number of alerts is a potential measure of efficacy.

- **Recognition Time**

A third important metric is the Recognition Time. Note that the actual amount of time taken to act on an alert will always be longer than the Recognition Time 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.

The Recognition Time 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 Recognition Time is to be fast enough to enable a real-time response.

6. Monitoring and review

The policy owner has overall responsibility for ensuring the content of this policy is appropriate and up to date. Review and amendments will be coordinated by the Policy Unit.

This policy will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use, and will be reviewed every 2 years as a minimum.

DCP are 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. DCP will implement a robust governance process to review the effectiveness and impact of their LFR deployments.

This policy pays due regard to the Equality Act 2010, including the Public Sector Equality Duty, in order to support the ethical and operational use of overt LFR within

the communities of DCP. This is addressed in the Equality Impact Assessment as well as further documentation as listed at section 2.6.

7. Associated documents

Policy and Procedure

- J-P-067 Alliance appropriate policy general processing GDPR
- J-P-069 Alliance appropriate policy law enforcement processing
- J-P-013 Alliance data protection policy
- J-P-011 Joint records management policy
- DCP-P-026 Stop and search policy
- DCP-OPr-041 Stop and search procedure

SharePoint

- Facial recognition
- Equality & Community Impact Assessments
- Force Purpose and Objectives
- Information Management: Data Protection, Freedom of Information, Records Management, Government Security Classification, Information Assurance, Information Sharing, Disclosure, Disclosure & Barring Service and Data Quality

College of Policing

- Code of Ethics
- Authorised Professional Practice

Other

- Police Race Action Plan
- NPCC Digital imaging and multimedia procedure v3.0
- Information Commissioner's Office (ICO): Facial recognition technology and surveillance
- ICO: The use of LFR technology in public places
- British Standards Institute: Guide to safe and ethical use of facial recognition tools launched
- British Standards Institute: Facial recognition technology – ethical use and deployment in video surveillance-based systems code of practice BS9347:2024
- Biometrics and surveillance camera commissioner – Code of practice and the 12 guiding principles
- Human Rights Legislation

8. Document history

Present portfolio holder: Assistant Chief Constable for Vulnerability & Crime

Present document owner: Chief Superintendent, Protecting Vulnerable People Command

Present owning department: Intelligence Directorate

Below details required for new documents, major amendments (Dorset only) or novel/contentious amendments (Devon & Cornwall only)

Name of Board and/or Chief Officer approving: Assistant Chief Constable for Vulnerability & Crime

Date approved: 09/07/2026

Business Board member approving (Devon & Cornwall only when not contentious or novel): Protecting Vulnerable People Commander

Date approved: 29/06/2026

9. Version history

Version: 1.0

Date: 13/07/2026

Reason for amendments: Creation of Live Facial Recognition policy

Amended by: Policy Manager, Deputy Director of Intelligence (DCP) and Intelligence Manager (Dorset Police)

We welcome any comments or suggestions you wish to share about the content or implementation of this procedure. If you would like to make contact to discuss further, please email:

Forcepolicyandprocedures@devonandcornwall.pnn.police.uk

Appendix A – Terminology

Adjudication

A human assessment of an alert generated by the 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.

Alerts

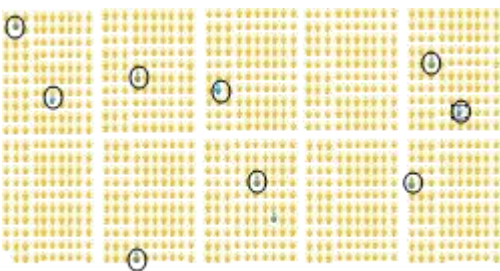
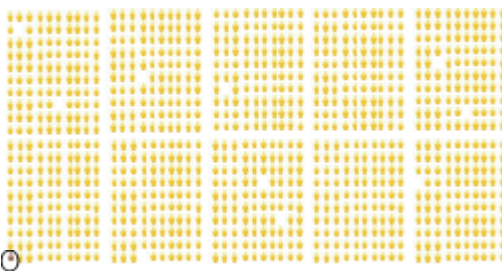
An alert is generated by the LFR application when a facial image from the video stream is being compared against the Watchlist and returns a comparison (similarity) score above the threshold. Types of alerts are:

- **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.
- **False Alert**
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.
- **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.

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 ISO:

	True Recognition Rate	False Alert Rate
What is it?	The total number of times individuals on a Watchlist pass through the Zone of Recognition and correctly generate 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 by the LFR system or not).	The number of alerts generated by individuals that are not on the Watchlist 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.
-----------------------	--	--

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.

Blue Watchlist

A Watchlist comprising of 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.

Candidate Image

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

Deployment

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

Deployment Record

A combination of output from 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:

- Location
- Dates and times
- Deployment and Watchlist rationale
- Legal basis
- Necessity
- Proportionality
- Safeguards
- Watchlist composition

- i) AO
- j) Resources
- k) Relevant statistics
- l) Outcomes
- m) Summary of any issues
- n) Threshold setting

Engagement

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

Environmental Factors

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

Faces per Frame

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

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.

Facial Recognition Technology

This technology works by analysing key facial features, generating a mathematical representation of these features (the Biometric Template), and then comparing that template to those of known faces in a database in order to generate possible matches. This is based on digital images (either still or from live camera feeds).

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.

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.

Person(s) of Interest

Person(s) on a Watchlist.

Possible Match

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

Probe Image

A facial image which is searched against a Watchlist.

Recognition Time

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

Similarity Score

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

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.

System Factor

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

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.

True Recognition Rate

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

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.

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.

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. 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.

Appendix B - Glossary of 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
LFR	Live Facial Recognition
NPCC	National Police Chiefs' Council
NPL	National Physical Laboratory
PIRM	Code of Practice for Police Information and Records Management
RT	Recognition Time
SWP	South Wales Police
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