Surrey & Sussex
Policing Together

Standard Operating Procedure (SOP) For the Overt Deployment of Live Facial Recognition (LFR) Technology

Protective marking:	Official - Sensitive
Publication scheme Y/N:	No
Title:	Standard Operating Procedure for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology
Version:	Version 1.1
Summary:	Establishes procedures for the Deployment of Live Facial Recognition (LFR) technology in support of policing operations.
Department:	
Review date:	01/12/2025

Version	Date	Authority	Evidence of approval	Record of change
0.1	09.05.2025	Project Lead	Ch. Insp [redacted]	Initial Draft
0.2	03.05.2025	Programme Director	Det. Ch. Sup [redacted]	First Review
0.3	17.09.2025	Project Lead	Ch. Insp [redacted]	Minor Amendments
1.0	10.10.2025	SRO	ACC [redacted]	No Amendments
1.1	10/11/2025	Programme Director	Det. Ch. Sup [redacted]	Minor Amendments

Contents

1 Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool.

2 Application

2.1 All Surrey/Sussex (SY/SX) police officers and police staff, including the extended police family and those working voluntarily or under contract to the Commissioner must be aware of, and are required to comply with, all relevant SY/SX policy and College of Policing Authorised Professional Practice (APP) on the subject.

2.2 This SOP applies to officers, staff, volunteers and specials in the following roles:

a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the planning and deployment of LFR technology

b) All police officers and police staff involved in any subsequent investigation resulting from the operational deployment of LFR technology

c) All Authorising Officers (AO)

d) The operational command team for any LFR Deployment (Gold, Silver and Bronzes)

e) LFR Operators and LFR Engagement Officers.

Note: This list is not intended to be exhaustive.

2.3 LFR Technology is just one of many different technological tools or systems that may be used by the Police operationally. The nature of modern policing is such that inevitably any one such technology or system is unlikely to be used in a complete vacuum alone. In the same way that a PC on patrol might simultaneously be deployed with a vehicle and a radio, it is likely that at any deployment of LFR other technologies will also be simultaneously present or used. Set out below are three examples of distinct and unco9nnected technology that may be used during the same time period of a deployment but are fundamentally separate systems independent of

LFR and whose compliance is handled separately.

Body Worn Video (BWV).

Officers and staff deployed on LFR operations will likely often be using BWV in line with the forces policy. BWV is an overt piece of technology, and its use is governed by the policy and other compliance documents found here Body Worn Video Policy (Surrey and Sussex) (1133).

Officers will switch their devices on in response to an alert and are on their way to engage with the person. The BWV will be left on until the conclusion of the interaction.

Policy further details when the BWV will be used to record. Users will not indiscriminately record entire duties or patrols and must only use recording to capture video and audio at incidents that would normally be the subject of electronic pocket notebook entries or as 'professional observation' such as stop/search, arrests, issuing of out of court disposal orders for example, whether these are ultimately required for use in evidence.

For further information about BWV please see the force policy at Body Worn Video Policy Surrey and Sussex (1133).doc

ANPR

Automatic Number Plate Recognition (ANPR) is a technology using cameras that automatically identifies number plates and converts the images of those number plates into the correct alphanumeric sequence of digits that number plate represents. This information is them recorded and processed in a database for law enforcement purposes. The LRF vans are equipped with ANPR technology. However, ANPR will not form part of the LFR deployment, the system will be turned off and not monitored for the purposes of an LFR deployment. The ANPR system will only be used when the

relevant vans are being used for purposes other than LFR deployments. The technology does not record individuals and only works from the vehicle's registration plates. Details of the forces use of ANPR can be found in the policy at Automatic Number Plate Recognition Surrey and Sussex Policy and Procedure.doc

CCTV on the LFR van.

In addition to the CCTV system that is a composite part of the LFR system, the LFR van has its own additional CCTV system that provides the operators of the vehicle with CCTV footage of the areas directly outside the van. It has a different field of vision to the cameras with the LFR technology, it does not use any LFR technology or can use LFR software.

These cameras are placed on the 4 corners of the van just above the door level to provide a 360-degree view of the outside of the van. They serve a different purpose to the LFR technology and are there for officer/safety of those in the van. The CCTV will be recording during the deployment for those purposes only and will be used and retained strictly in line with the relevant policies and governance documents including the LRF policy and procedure[1] [Insert link here]. Details of the forces use of CCTV can be found in the policy and governance documents at [Insert links here].

3 Terminology

3.1 This SOP focuses exclusively on LFR. Terminology relating to LFR is defined in the SY/SX Policy for the Overt Deployment of Live Facial Recognition Technology Document[2].

4 Authority to Deploy LFR

[1] Live Facial Recognition | Sussex Police
Live Facial Recognition | Surrey Police
[2] Live Facial Recognition | Surrey Police and Live Facial Recognition | Sussex Police

4.1 In normal circumstances the authority given by an AO to deploy LFR in support of a policing operation should be made by an officer not below the rank of Superintendent. Their authorisation should be recorded in writing.

4.2 The SY/SX LFR Application / Written Authority Document recognises that the intelligence case(s) 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. Where the SY/SX LFR Application / Written Authority Document is to be used to authorise a single period, and the dates will be detailed as part of the authorisation.

4.3 Prior to AO authorisation and the Deployment of LFR in public spaces, several documents must be completed and an SY/SX officer of NPCC rank[3] must be engaged by the AO. Whilst 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 pan-SY/SX issues are considered as much as possible. However, each force will act as a separate data processor. This affords NPCC the opportunity to veto the deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

4.4 Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable.

4.5 The authority of the AO:

a) Must articulate the legitimate aim(s) of the Deployment and the legal powers that are being relied upon to support the Deployment

b) Must record in summary the basis on which the AO is satisfied that the Deployment complies with SY/SX LFR documents, or is otherwise authorised and sets out the exceptional reasons for doing so

c) Must, from a Human Rights Act 1998 perspective, articulate (i) how and why the Deployment is necessary (and not just desirable), and (ii) is proportionate to achieve the legitimate aim(s) of the Deployment

d) From a Data Protection Act 2018 and UK GDPR perspective, articulate how it is complaint with all the relevant requirements in this regard (for example this could include why the proposed deployment is strictly necessary for the SY/SX's law enforcement purposes; meaning there is a `pressing social need' and it is not reasonably viable to address this through less intrusive means, either because less intrusive tactics have been tried, or it is reasonably believed that those tactics are unlikely to be effective) details of the applicable requirements are set out in both the LFR DPIA and the LFR Legal Mandate for reasons of substantial public interest; and / or

i. Necessary for the administration of justice; and / or

[3] NPCC –`NPCC rank' denotes an officer holding the rank of ACC or above.

ii. Necessary for the safeguarding of children and/or of individuals at risk; and

iii. Necessary notwithstanding any expectations 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

e) Articulate that the AO has given regard to the safeguards proposed for the deployment and the safeguards contained within the SY/SX LFR documents, and having done so considers that the deployment in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the Data Protection Act 2018 and UK GDPR as well as in light of their obligations under Public law etc; and

f) Specify that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the watchlist complies with SY/SX LFR Documents, including the legality, necessity and proportionality criteria

g) Articulate any authority to include additional categories of persons to the watchlist, including the basis on which this is done including how the legality, necessity and proportionality criteria have been met, in addition to those included to meet the purpose of the deployment; and

h) must include a direction from the AO that 1) all police officers / staff engaged as operators in the deployment must have received SY/SX LFR training as per the SY/SX LFR documents, and 2) all Officers involved in the deployment must have received a pre-deployment briefing

i) Required to include a statement confirming that in the context of this deployment the AO considers that the Deployment is proportionate with the benefits anticipated from the use of LFR being such as to outweigh the concerns and impacts there may be in relation to people's human rights and rights relating to equalities

j) Set out confirmation that in the context concerned the AO is satisfied that the control measures set out in the Data Protection Impact Assessment, Community Impact Assessment, and Equality Impact Assessment have been reviewed and considers the specific measures proposed to be applied to be appropriate mitigants for the relevant deployment.

k) Articulate the minimum threshold setting to be utilised during the deployment as determined by the AO (and the basis for that determination). Ordinarily this setting will be equal to or above the value where no FRT System bias is detected (0.64 with the current FRT algorithm used by SY/SX). The Threshold value may be lowered based on the intelligence case with a full rationale detailed in the

4.6 In cases of urgency the Force Gold Command structure may authorise the deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency.

4.7 Situations where the need for an authorisation to be granted urgently would include:

a) an imminent significant threat-to-life or of serious harm to people or property; and / or

b) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which, having considered this against the impact of the deployment on individuals and the public generally, supports the urgency of action.

c) the same safeguards will be applied to the application as those applied to a preplanned operation.

4.8 If an authorisation is given under the urgency criteria above, it shall be the duty of the AO who gives it, to inform an officer of the rank of Superintendent or above as soon as practicable, that LFR has been deployed and the reasons why alongside the considerations considered. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

4.9 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.

5 'Where' - Date, Time, Duration and Location of Deployment

5.1 The AO should define the date, time, location and duration the deployment (and urgent deployments) 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.

Considerations relevant to a LFR Deployment location

The intelligence case, policing purpose to include a person on a watchlist, Community Impact Assessment and the environmental factors relevant to a potential deployment location will substantially inform the potential locations for LFR deployments as well as the set up in any location.

5.2 Deployment locations and watchlists have an inherently interconnected dependency. Having built a watchlist for a proposed deployment it will be

necessary to identify a potential deployment location. To be a valid deployment location it must be a place where for each person on the watchlist there are reasonable grounds to suspect that they may attend that place at the time or times at which the deployment will take place. Consequently, it will at times be necessary to either adjust the watchlist makeup or look for an alternative location for the deployment if there aren't reasonable grounds for suspecting that one or more of the persons on the original watchlist might attend that location. The reasons for any selected Deployment location (and the set up within that location) should be recorded and be capable of being considered and evaluated by an objective third person.

5.3 The selection of a particular deployment location may further be supported by:

a) 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

b) The location needs to take into consideration the Health and Safety of the public in the vicinity of the operation and officers/staff involved. It will also consider the ability for members of the public to choose not to walk in the zone of recognition. The location cannot be one that funnels the public to have to walk past it. It also needs to provide enough space for the engagement officers to be able to stop the person following an alert.

5.4 When reviewing a potential deployment location, AO's must also consider those who are likely to pass the LFR System

a) Those who are likely to pass the LFR System at that location

b) The reasonable expectations of privacy the public may have at that location (including the following considerations in particular)

i. That some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy Zone 1 central London thoroughfare being typically different to a quiet suburban park or backstreet

ii. The number and type of cameras used by the LFR System should also be considered in this context to ensure the nature, size and scale of the deployment enables those on a watchlist to be effectively located without disproportionately processing biometric data

c) Whether a proposed deployment location attracts concerns by reference to those persons expected to be at a particular location[4]:

[4] Should a deployment be necessary at a site that is focused on children (for example outside a school), signage and information about the LFR Deployment should typically be reasonably accessible to children who may pass through the Zone of Recognition. Consideration is needed as to the nature of the Deployment and data processing that is proposed and the effectiveness of the mitigations when assessing if a Deployment can be considered proportionate or not.

i. 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.

5.5 Where it is practicable to identify a person as being responsible for a proposed deployment location (as a whole or of a part of it), and where the area that person is responsible for raises a greater expectation of privacy. Then consideration should be given to liaising with that person as part of a community impact assessment process. For example, this might be the Headteacher of a school or the relevant official of a place of worship that are adjacent to a deployment. The involvement of the AO in this process should be sought where appropriate.

5.6 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 location and whether the aims being pursued could be similarly achieved elsewhere or by other means (such as by adapting the setup of the deployment). In instances where that location is *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 in line with the relevant LFR policies. This is to ensure the policing action proposed is necessary and not disproportionate to the aim being pursued.

Measures during an LFR Deployment

5.7 Save in exceptional operational cases the public should always be notified of LFR deployments in advance using force websites and other appropriate communication channels (including social media). However, in exceptional cases, where it is compliant to do so, such notification does not need to take place if and were doing so would undermine the objectives or operational imperative of the deployment (for example, in cases of urgency or where it would compromise other policing tactics).

5.8 Measures should also be taken during the deployment to ensure the policing presence is overt such that the public can both establish that LFR is being used and understand the nature of the data that is being processed. In addition to the use of uniformed officers and police marked LFR camera assets and vehicle, other steps for applicants to consider in the context of their proposed deployment location include the use of signage placed in sufficiently 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 policing tactic will also be relevant if the policing need to deploy is to be realised. For example, a deployment seeking to protect a site, or in a particular event may merit multiple levels of signs and the proactive distribution of leaflets to deter those with mal intent.

5.9 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. This document exclusively covers the overt deployment of LFR where it will always be a voluntary matter whether any individual wishes to pass through the zone of recognition or not. SY/SX staff deployed to such LFR operations must, as always, be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.

5.10 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 (add links to websites) should be provided with contact information for the SY/SX LFR operational team (LFR@Surrey.Police.uk and LFR@Sussex.Police.uk)

6 'Who' - Watchlist Generation and Criteria for an Image's Inclusion on a Watchlist

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

a) Safeguards relevant to all watchlists – including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics.

b) Who may be added to a watchlist – including in relation to police-originated, and non-police originated imagery.

Safeguards relevant to all Watchlists

6.2 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 SY/SX 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 specific policing need/s and be based on a credible and reasonable intelligence case The intelligence case must be current and crucially must be reviewed before each Deployment (including at least one review within the 24 hours prior to	This intelligence-driven approach ensures that the make-up of the watchlist is reflective of, and for the purpose of the LFR deployment, has a lawful purpose and follows the principles set out in our legal mandate

the deployment).	
Images sources: Police must be reasonably satisfied that images for use in watchlists are lawfully held by police with consideration also being given as to: • The legal basis under which the image has been acquired and the legal basis for the ongoing processing of that image since it was acquired • 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.	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 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 with the relevant requirements. 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 • 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 a false positive alert should a non-recent 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	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. To achieve this the watchlists will be restricted geographically for certain crime types and where a person is sought for a crime of significance this could mean across both Surrey and Sussex counties. 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 SY/SX SRO for LFR has determined the 1:1000 false alert rate represents an approach which balances these factors in a proportionate way.

proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);	
Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the deployment and must always be subject to a final check for currency and compliance with the requirements of the law and LFR documentation before the importation.	This is to ensure the ongoing accuracy of a Watchlist should a deployment be necessarily undertaken for a period of longer than 24 hours
Watchlist design: Watchlists should be segregated into different categories of sought person and technical measures implemented that make the reason for inclusion on a watchlist clear to the operator in the event of an alert.	This is to ensure the status of those on a watchlist is recognised by those involved in undertaking engagements to ensure the appropriate action is taken should an alert be generated (because for example the position will be very different between engaging someone who is wanted because they are a missing vulnerable person as opposed to a person subject to an arrest warrant for previously resisting arrest.

Additional safeguards relating to protected characteristics

6.3 Following on from the *Bridges case*, in December 2020 the then 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 SY/SX in this document reflect the SY/SX LFR System's performance and SY/SX's particular use- cases for LFR.

6.4 SY/SX has confidence in the LFR System's performance, particularly in relation to gender, age and race. The LFR software has been tested by the National Physical Laboratory.

6.5 SY/SX recognises that *regardless* of performance considerations, it should take particular care when considering and publishing details (We will follow standard UK media law when publicising any outcomes from LFR deployments i.e. age, gender, town and offence for an arrest. Those under 18 years old are granted automatic anonymity.) 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:

a) There may be different privacy expectations around the use of LFR[5] and that these can be particularly relevant in relation to these people given their potential vulnerability[6] (for example a person may have undergone a gender reassignment in the time between when a photo was taken that then is subsequently used on a watchlist, and the time when that person may be identified for further engagement after a match on LFR).

6.6 Documenting composition: SY/SX provides that each deployment must specifically identify and document whether the watchlist contains persons who are believed or suspected to be:

a) aged under 18-years-old.

b) aged under 13-years-old.

c) a person with a relevant disability[7].

d) 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.

6.7 Safeguards regarding composition: The following outlines some of the further, specific safeguards that apply to the composition of the watchlist:

[5] For example, in relation gender reassignment, see Section 22 of the Gender Recognition Act 2004 which protects disclosures other than in certain specific circumstances which include where the disclosure is necessary for the purposes of preventing or investigating crime.

[6] For example, in relation to children, see: **https://www.app.college.police.uk/app- content/detention-and-custody-2/detainee-care/children-and-young-persons/#children-and- young-persons** which is in the context of detention and custody but notes children and young people are a protected group with specific vulnerabilities. Their treatment in detention is governed not only by domestic legislation but also by the **UN Convention on the Rights of the Child (UNCRC)**

[7] A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) and that such a disability may impact on the performance of the police force's LFR system. Examples which may have an impact (depending on the performance characteristics of the specific LFR system) include if the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised.

	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[8]	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 SY/SX LFR Documents and the law 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.			
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 such as where shorter subjects may otherwise be blocked from the camera's line of sight.	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 decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		

[8] Generally, studies [https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf] have shown that young children, up to the age of 13 are both harder to correctly recognise (lower True Positive Identification Rate) but also harder to distinguish between (higher FPIR). The higher FPIR may lead to more False Alerts being generated against young children if there is an image of a young person in the Watchlist.

Police-originated images that may be included on a Watchlist

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

a) Wanted by the courts

b) 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

c) Subject of bail conditions, court order or other restriction that would be breached if they were at the location at the relevant time; *and/or*

d) Subject of information or intelligence that would lead to suspicions of an immediate threat to life

e) Subject of information or intelligence that would lead to suspicions of an Immediate risk of serious harm **-** including safeguarding the welfare of vulnerable people, including children at imminent risk of abuse or otherwise harmed.

6.9 Where persons are included based on bail conditions, court order or other restriction, whether imposed in a criminal court or otherwise, several considerations need to be made before inclusion. Inclusion on this basis must be assessed against various factors including:

a) The risk posed by that individual

b) The ability of officers to check and enforce conditions (for example, conducting checks on a mobile phone of a person subject of a Serious Crime Prevention Order)

c) The proportionality of inclusion in a Watchlist. An example of this would be an including on a watchlist a person subject to bail conditions preventing that person from attending a particular shopping location, because LFR is being deployed there in such a way that the person would only trigger an alert if they were in breach of the condition. That would be a legitimate and a proportionate inclusion. In contrast if the person was subject to a bail condition that only prohibited entry to a specific store in that shopping location, then including them on a watchlist for a deployment where that person could legitimately trigger the system without having first breached the condition (because they were in the public area and never entered the shop) would not be proportionate or legitimate.

The AO must be satisfied that the individuals included in this watchlist have been assessed and that the conditions have been lawfully imposed and remain in effect

at the time of the deployment.

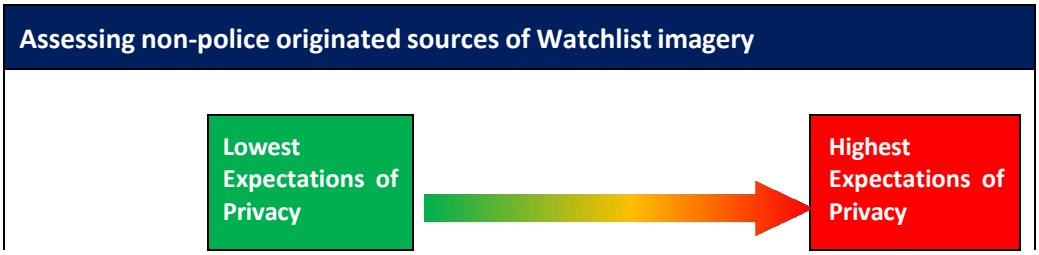
Subjects considered for inclusion will be assessed on an individual basis by their Offender Manager or the Investigating Officer. Not every individual who is subject of conditions will be included in watchlist and the conditions as well as the individual must be relevant, proportionate and necessary in terms of the deployment taking account of those persons legal rights. SY/SX will take reasonable steps to communicate with persons who may be included in this category and provide them with information relating to the use of LFR in a policing context.

6.10 Where police originated images other than custody images are considered for use, additional consideration regarding the inclusion of such images is needed. Consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a watchlist to meet a policing objective and the proportionality of using such images on an LFR System. It may be more challenging to meet the data protection requirement that such further LFR processing of such images is 'fair' if they were originally obtained for another purpose. For example, if an individual supplied a family photo 5 years ago to help police locate a missing grandparent on the explicit basis it would be used for the search and then deleted, but for some reason the photo was never deleted after the grandparent was found, and the Police then sought to use that image to locate another individual in the family photo and wanted to use the image for an LFR watchlist this is unlikely to be fair or compliant.

Non-police originated sources of Watchlist imagery

6.11 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 SY/SX 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. For the avoidance of doubt, this policy does not provide a basis to proactively acquire images solely for use on an LFR Watchlist.

6.12 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'.



Imagery	Layer A Layer B Layer C

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 because of a lawful power of search or seizure. • 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.

Image Layer	Outline
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.

6.13 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 at paragraph 6.11 above.

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

a) Wanted by the courts

b) 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

c) Subject of bail conditions, court order or other restriction that would be breached if they were at the location at the relevant time; *and/or*

d) Subject of information or intelligence that would lead to suspicions of an immediate threat to life

e) Subject of information or intelligence that would lead to suspicions of an Immediate risk of serious harm **-** including safeguarding the welfare of vulnerable people, including children at imminent risk of abuse or otherwise harmed

6.15 **'Wanted by the courts**.' This term includes those with outstanding arrest warrants or who are otherwise subject to a relevant legal obligation imposed by a court (usually to attend). 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.

6.16 '**Missing persons.'** This term will be subject to the College of Policing definition of medium risk (or above) that is contained in the Missing Persons APP[9], meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should consider the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.

6.17 **'Immediate threat to life; *and/ or* Immediate risk of serious harm - including safeguarding the welfare of vulnerable people, including children at imminent risk of abuse or otherwise harmed'.** This ground will reflect that inclusion in a watchlist is necessary is to locate the person to the manage risk of serious harm or an imminent need to safeguard an individual ensure their continued welfare.

6.18 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

[9] Missing persons | College of Policing

as to how the individual or group of individuals[10] present(s) a risk of harm to themselves or to others and:

a) how using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*

b) why the significance of the harm identified means it is **necessary** for the police to act to manage the risk.

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

a) 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

b) The importance of locating the person or people sought with reference to the threat, harm and risk[11] which the addition to the Watchlist addresses.

c) The significance of the threat, harm and risk identified, which inclusion on the watchlist would address outweighs any expectations of privacy.

SY/SX LFR Documents

6.20 Assessments: For each authorised LFR operation, the following assessments need to be considered and amended where necessary:

a) Data Protection Impact Assessment* (Review/Amend/Adopt)

b) Equality Impact Assessment* (Review/Amend/Adopt)

c) Community Impact Assessment* (Review/Amend/Adopt)

d) The Surveillance Camera Commissioner's Self-Assessment* (Review/Amend/Adopt)

7 Management of Risk & Resource Levels

7.1 Each deployment should be risk assessed in line with SY/SX 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

[10] A group of individuals may be added to the watchlist where everyone within the group meets a criterion that would justify addition to the watchlist.

[11] Including for the purposes of taking preventative measures against the occurrence (or future occurrence) of the relevant threat, harm and risk.

use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the deployment, timing, community tension, the likely make up of the group of the public that will pass through the location, and any other factors that appear relevant.

7.2 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 considering the relevant circumstances. For example, scenarios where LFR deployment might increase the risk of public disorder are likely to require greater officer presence and support than other deployments.

7.3 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.

7.4 All SY/SX officers and staff deployed on LFR Deployments must be compliant and in date with SY/SX First Aid and where applicable officer safety (PPST) training requirements. All SY/SX officers and staff involved in an LFR Deployment must receive an LFR briefing prior to deployment.

8 Planning & Booking

8.1 As part of the LFR planning process and before the AO authorises a deployment, the SY/SX LFR team should be consulted on the appropriateness and viability of a deployment.

9 LFR Operational Roles

LFR Command Team

9.1 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:

a) 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.

b) Silver Commander (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 regard to the effectiveness of the safeguards in place whilst LFR is being used.

c) 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.

9.2 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.

LFR Operator

9.3 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.

9.4 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.

9.5 The LFR Operator's log should include:

a) 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

b) What decision was taken regarding whether to engage a member of the public or not

c) Whether an engagement was successfully undertaken, and the outcome of the engagement.

LFR Engagement Officer

9.6 LFR Engagement Officers must understand 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 must be deployed in uniform. They are responsible for

community engagement and developing confidence in our communities for the use of LFR.

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

9.8 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[12]. 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 potential factors influencing the generation of an alert, such as those relating to the system and its setup, to the subjects of the system and to the environment of the deployment.

9.9 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 (separate to any LFR matching that had taken place prior to the engagement).

9.10 Whilst officers must exercise their own discretion when using their powers of arrest and detention, SY/SX 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. 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. Fundamentally engagements should be no different whether the intelligence that led to the engagement taking place was an LFR match or was something else such as a witness statement, independent and sufficient checks need to be made.

9.11 If an engaged individual cannot be identified or fails to confirm their identity,

[12] The driving force behind this point is that an LFR Operator should not be making the decision that an Engagement Officer carries out an Engagement. The Operator provides intelligence in the form of information relating to a match, they must not direct the engagement officers to do any particular action. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own `reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take relating to a match, they must not direct the engagement officers to do any particular action. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own `reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take.

this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be able to justify the use of any powers, any action taken, and have a lawful basis for doing so.

9.12 After any engagement (that follows an alert), the LFR Engagement Officer must update the LFR Operator with the outcome of that engagement.

9.13 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 (where they independently have both a lawful basis and lawful power and it is right and proper to do so) 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

10 Post-Deployment

10.1 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.

10.2 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.

10.3 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):

a) Total number of individuals and the total number of images included in the Watchlist (there may be multiple images of some individuals)

b) 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)

c) Total number of LFR application-generated alerts

d) Total number of alerts that do not result in an Engagement; and

e) Total number of Alerts where a decision was taken to Engage an individual

f) Total number of Alerts that are confirmed as true alert (the individual

is who the LFR application suggests are)

g) Total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are)

h) Total number of correct alerts that result in an engagement that do not require any further police action

i) 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

j) Threshold setting for the deployment

11 LFR Application Security

11.1 The LFR application includes several physical and technical security measures. These include:

a) Images are transferred onto the LFR application via an encrypted USB device

b) The LFR application is a fully closed system with two layers of password protection to access the application

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

d) Role based access controls with limited user permissions are implemented on the LFR application

e) A full audit is maintained of all user-initiated actions undertaken during a Deployment; and

Technical issues with the LFR application follow a structured support process model that includes escalating issues to the vendor if required.

12 Data Retention & Data Management

12.1 The SY/SX must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the SY/SX LFR Documents. This means that:

a) The LFR application does not generate an alert, that a person's biometric data is immediately automatically deleted

b) 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.

12.2 Where the LFR application generates an alert, all personal data is deleted as soon as practicable and in any case within 24 hours.

12.3 All CCTV footage generated from LFR Deployments is deleted within 24 hrs, except where retained:

a) In accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996

b) In accordance with the SY/SX's complaints / conduct investigation policies.

c) 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.

d) In accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 24 hrs will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

e) 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 SY/SX Data Protection Officer.

Register of Deployments

12.4 Any Deployment of LFR must be recorded on a centrally held register. This register will record several things including:

a) Name and rank of the AO and command team

b) Date, Time, Duration, and Locality of Deployment

c) Watchlist composition statistics (not including any personal data); and

d) The number of alerts, broken down as True Alerts and False Alerts including:

i. perceived age range

ii. perceived sex

iii. perceived race

e) number of Engagements and their results.

12.5 The SY/SX will make information relating to LFR Deployments available to the public in accordance with the SY/SX LFR Documents. This information is available on the force website.

13 Contact Information

13.1 The SY/SX LFR team can be contacted using the following email addresses; LFR@Surrey.Police.uk and LFR@Sussex.Police.uk.

14 Further Documentation

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

a) Information Management APP.

Information management | College of Policing

b) National Decision Model.

National decision model | College of Policing

c) National Intelligence Management.

Intelligence management | College of Policing

d) College of Policing Code of Ethics.

Guidance for ethical and professional behaviour in policing | College of Policing

e) Home Office Biometric Strategy – Published June 2018; www.gov.uk/government/publications/home-office-biometrics-strategy

f) High Court Ruling – R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin); High Court Judgment Template