Protective marking:	Official
Publication scheme Y/N:	No
Title:	Standard Operating Procedure for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology
Version:	Version 2.0
Summary:	Establishes procedures for the Deployment of Live Facial Recognition (LFR) technology in support of policing operations to locate those on Watchlists.
Branch/ OCU:	MPS LFR
Review date:	29th November 2022

STANDARD OPERATING PROCEDURE (SOP) FOR THE OVERT DEPLOYMENT OF LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY

Terms & Definitions: Capitalised terms used in this LFR SOP shall have the meaning given to them in the MPS LFR Policy Document unless otherwise defined in this LFR SOP.

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 an overt way to locate those on Watchlists and in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool. As part of a published suite of documents, this also allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the Metropolitan Police Service (MPS), as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

To help set the standard operating procedures in context, a summary flowchart has been produced and is annexed to this SOP. It shows the various stages required to plan for and deliver an LFR Deployment.

2 Application

2.1 All MPS police officers and police staff and those who support the extended police family (including those working voluntarily or under contract) must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.

2.2 This SOP applies in particular to officers and staff in the following roles:-

a) All operational officers (both uniform or detective) and police staff and their supervisors involved in the planning and Deployment of LFR technology; *and*

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

c) All Authorising Officers (AO); *and*

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

e) LFR Operators and LFR System Engineers.

Note: This list is not intended to be exhaustive.

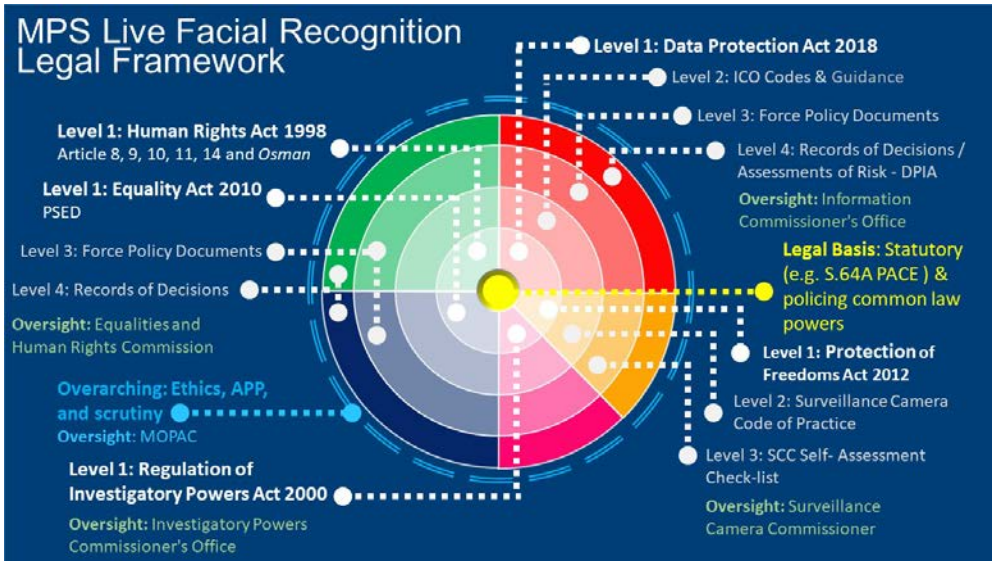
3 Terminology

3.1 This SOP focuses exclusively on LFR**.** Terminology relating to LFR is defined in the MPS LFR Policy Document.

4 Authority to Deploy LFR

The legal framework to Deploy LFR

4.1 The legal framework, which underpins the application and authority process to deploy LFR, is set out in the MPS LFR Mandate. How that framework comes together is also summarised in the schematic below in order to assist applicants and decision makers:



4.2 The legal framework schematic is best read from the inside of the diagram out in the following way:

Legal Framework Schematic Key:	
Yellow centre	This is the legal basis for the action – i.e. the legal power(s) that supports the compilation of the Watchlist and the use of LFR.
Red segment	This area reflects that biometric and other personal data is processed by the LFR system. It reflects the application of the Data Protection Act 2018 and underlying documents that govern and reflect this.
Green segment	This area reflects the relevance of human rights to the use of LFR. Some, like the right to privacy, will be engaged by those on the LFR Watchlist and/or passing the LFR system. The engagement of other rights will be context dependant.
Blue Segment	This area reflects the relevance of equality considerations and the application of the Public Sector Equality Duty. It shows the underlying documents which also govern and show compliance with this duty.
Pink Segment	This area reflects the potential application of the Regulation of Investigatory Powers Act 2000 (RIPA). For an overt capability, it is important to have regard to RIPA to ensure the use of LFR does not become directed surveillance.
Orange Segment	This area reflects that LFR uses CCTV cameras to film those passing through the Zone of Recognition as part of the wider LFR system. It recognises the relevance of the Protection of Freedoms Act 2012 to CCTV in public spaces by policing in England and Wales.
Level 1	**Primary legislation:** This level of the legal framework reflects a statutory legislation enacted by Parliament that combines in its application to provide a framework for the regulation of LFR.
Level 2	**Secondary legislative instruments:** This level of the legal framework reflects statutory codes and non-statutory guidance typically issued at a national level which Chief Officers should have regard to when seeking to apply the Level 1 legal framework. Authorised Professional Practice (APP) issued by the College of Policing also sits at this level within the legal framework. However, given some APP is not specific to a particular area of primary legislation, it is reflected as an overarching consideration in the legal schematic to reflect its pervasive application.
Level 3	**Force policy:** This reflects policy documents issues at a force level. They provide for the operational implementation of the legal framework in a way that helps the use of LFR to be both accessible and foreseeable to the public.
Level 4	This level of documentation reflects the use of the legal framework in practice – ensuring relevant decisions, including the rationale, necessity and proportionality for use is recorded. It is also the place where decisions of relevance to the Public Sector Equality Duty should be recorded.
Overarching:	The all-encompassing blue dashed line shows that there are a number of aspects to the lawful and ethical use of LFR systems which are pervasive and do not just relate to one area of law.

Applying to Deploy LFR

4.3 An applicant may seek the authorisation to deploy LFR via the MPS LFR Form 1, Part 1 – Application. The MPS LFR Form 1 is annexed to this SOP to assist readers with the requirements to apply for and authorise an LFR Deployment.

4.4 In normal circumstances the authorisation 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 via the MPS LFR Form 1, Part 2 – Written Authority Document.

4.5 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an MPS officer of NPCC rank[1] must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-London issues are taken into account as much as possible. 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.

4.6 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 via the MPS LFR Form 1, Part 2 – Written Authority Document.

4.7 Should a further law enforcement purpose be identified after the AO has issued their authorisation 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.

4.8 Urgency: In cases of urgency an officer below the rank of Superintendent, but not below the rank of Inspector, 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. All authorisations must comply with the requirements set out in paragraph 4.3.

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

a) an imminent 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 supports the urgency of action.

4.10 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. It is for the

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

Superintendent (or higher-ranking) to then authorise the Deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

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

5.1 The AO should define the date, time, location and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment.

Considerations relevant to a LFR Deployment location

5.2 The intelligence case, policing purpose to include a person on a Watchlist and Community Impact Assessment will substantially inform the potential locations for LFR Deployments.

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

5.4 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 at a Deployment location; *and*

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

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

a) **the reasonable expectations of privacy the general public may have as a whole at that location**:

i. 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; and

ii. the number of cameras used by the LFR system should also be considered in this context to ensure the size and scale of the Deployment enables those on a Watchlist to be effectively located without disproportionately processing excessive biometric data; *and*

b) **if a proposed Deployment location attracts particular concerns by reference to those expected to be at a particular location**[2]**:**

[2] 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

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.

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

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

Measures during an LFR Deployment

5.8 During <u>any</u> policing operation where LFR is Deployed in line with SOP, signs publicising the use of the technology should be prominently placed in advance (outside) of the Zone of Recognition. These measures are to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition.

5.9 The public should also be notified of LFR Deployments in advance, save in exceptional cases where doing so would undermine objectives or operational imperative of the Deployment (for example, in cases of urgency or where it would compromise other policing tactics). Details of the LFR Deployment are to be notified to the public using force websites and other appropriate communication channels (including social media).

5.10 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. MPS staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.

5.11 Any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. Any person who requires further information relating to LFR should be provided with contact information for the MPS LFR operational team (LFR@met.police.uk).

---

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.

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;

c) The approach to be taken to Additional Watchlist Categories – this being relevant where the need to undertake a Deployment is already made out by reference to the primary Watchlist and the intelligence case supports the use that the Deployment to locate further persons, for example those wanted by the courts - such additional purpose must also be necessary and proportionate.

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 MPS 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
1.	**Intelligence**: Watchlists must be driven by a policing need and based on the intelligence case The intelligence case must be current and reviewed before each Deployment.	This intelligence-driven approach ensures that the make-up of the Watchlist is honed to, and not excessive for the purpose of the LFR Deployment
2.	**Images sources**: Watchlists must only contain images lawfully held by police with consideration also being given as to: • the legal basis under which the image has been acquired; and • the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.	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. Additionally policing has a responsibility to

	Requirement	Rationale for the requirement
		avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.
3.	**Image selection**: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: • is of a person intended for inclusion on a given Watchlist; and; • is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR system generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR system to operate within the 1:1000 False Alert Rate using the propose image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);	This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that person should they pass the LFR system. This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The MPS SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.
4.	**Watchlist currency**: Watchlists must not be imported into the LFR system more than 24 hours prior to the start of the Deployment.	This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours
5.	**Watchlist design**: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated

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 the MPS in this document reflect the MPS LFR system's performance and the MPS's particular use-cases for LFR.

6.4 The MPS explains how it has confidence in the LFR system's performance, particularly in relation to gender and race in its published document, the Metropolitan Police Service Live Facial Recognition System; Understanding Accuracy and Bias

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

a) There may be different privacy expectations around the use of LFR[3] and that these can be particularly relevant in relation to these people given their potential vulnerability[4].

b) The MPS recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.

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

c) aged under 18-years-old;

d) aged under 13-years-old;

e) a person with a relevant disability[5];

f) 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.

---

[3] 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.

[4] 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)**;

[5] 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.

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

	Age (U. 18)	Age (U.13)	Disability	Gender Reassignment
Circumstances				
	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 18-years-old	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old[6]	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 the MPS LFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images		There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.		
Legal Advice		Specific advice must be sought from the Directorate of Legal Services and the MPS LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		
Technical Advice		Regard should also be had to consider System and Subject Factors and the ability for the LFR system to generate an accurate Alert against the image proposed for inclusion on the Watchlist. Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		

[6] 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 custody images of individuals and/or police originated images other than custody images of people who are:-

a) wanted by the courts; *and/or*

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; *and/or*

c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or*

d) missing persons deemed increased risk; and/or

e) presenting a risk of harm to themselves or others; *and/or*

f) who are a victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual and that individual themselves would fall within paragraphs (a) – (e).

6.9 Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such 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 in order to meet a policing objective and the proportionality of using such images on an LFR system.

Non-police originated sources of Watchlist imagery

6.10 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 the MPS 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.

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

Assessing Non-police originated sources of Watchlist imagery	

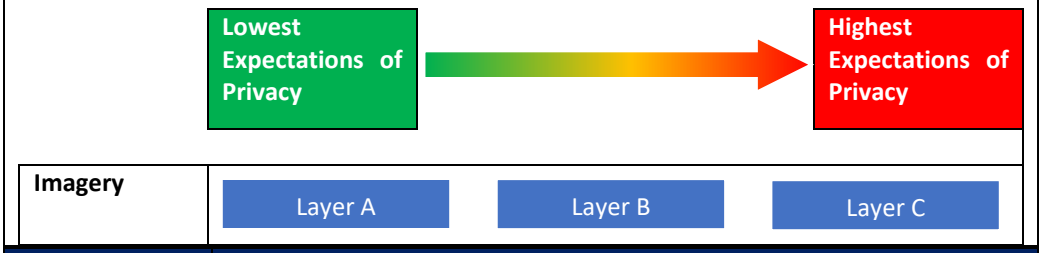



Image Layer	**Outline**
Non-police originated image – **Layer A**	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images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

6.12 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 6.9 above.

6.13 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; *and/or*

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; *and/or*

c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or*

d) missing persons deemed increased risk; and/or

e) presenting a risk of harm to themselves or others; *and/or*

f) who are a victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual and that individual themselves would fall within paragraphs (a) – (e).

Interpretation of Watchlist categories

6.14 **'Missing persons deemed increased risk.'** This term will be subject to the College of Policing definition of medium risk (or above) contained in Missing Persons APP. That is 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.

'Presenting a risk of harm'. Mitigating the risk of harm will need to have a legal basis for action under a policing common law power. 'Harm' can include a risk of harm arising in relation to a person's welfare and/or a financial harm including as a result of fraud or other dishonesty. It can also include 'Harm' in the context of posing a risk to national security.

6.15 The risk of harm will be informed by the intelligence case. This will need to inform the AO as to how the individual presents a risk of harm 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 take action in order to manage the risk.

6.16 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 sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;

c) how the need to address significance of the harm identified outweighs any expectations of privacy which attach to the Watchlist addition.

'Victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual'. This criteria includes a victim, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within paragraphs 6.8 (a) – (e) and 6.10 (a) – (e) of the categories that may be deemed appropriate for inclusion within an LFR Watchlist. The threshold for any Watchlist inclusion is high and the use of the category will be by exception; the necessity for inclusion must be based on a specific intelligence-case with the need for the inclusion on a Watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to able to demonstrate to the AO's satisfaction:

a) why the inclusion of each victim, person reasonably suspected of having information, or close associate is **necessary** to help locate the person who is wanted by the courts and/or the police; *and/or*

b) why locating each victim, person reasonably suspected of having information, or close associate person is **necessary** to advance the policing investigation; *and/or*

c) why locating each victim, person reasonably suspected of having information, or close associate is **necessary** to ensure their safety and/or the safety of others

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

d) 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

e) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;

f) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any

inclusion on the Watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others.

6.18 The then Surveillance Camera Commissioner recognised the need for policing to locate victims, witnesses and close associates via LFR in his November 2020 guidance, 'Facing the Camera'.[7] In this light, to assist MPS personnel and the wider public understand and foresee how this category may be used, the following are illustrative examples of where the need to add a person to a Watchlist under this category may be made out. In considering these examples, it from a MPS perspective, it is also important to consider any use of LFR in line with the MPS's strategic objectives for LFR.

Status	Example Circumstances
Victim	Intelligence supports an assessment that a victim of crime is under a continuing clear threat to their welfare. Other less intrusive efforts to locate them have failed or are unviable in the time available and there is a need to locate them for their own safety.
Person reasonably suspected of having information	The angle of the only CCTV from a violent gang-related knife attack does not show the faces of the perpetrators who remain at large. The footage does however show the faces of others who are reasonably considered to have seen the attack and it is clear that they should have had a good line of sight of it. If those people who are considered to have seen the offence can be located and they are assessed by the MPS as having relevant information that could be vital to progress the investigation, their location could help bring violent offenders who present a risk to society to justice.
Close associate	The MPS has received information that a person wanted for a serious sexual assault has been receiving phone calls from a close associate. They are using public phone boxes to remain in contact and support the perpetrator whilst they hide from the police. MPS has established that the close associate is not residing at their last known address and has been unable to otherwise locate them.

Additional Watchlist Categories

6.19 It may also be appropriate to include Additional Watchlist Categories into a Watchlist, in addition to those included in a Watchlist to meet the primary purpose of the Deployment. These Additional Watchlist Categories can comprise:-

[7] See paragraph 4.49 at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

a) Those with outstanding arrest warrants or are otherwise required by the courts within the MPS area.

The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general. In such circumstances, and noting that this is limited to those wanted by the courts within the MPS's area of operation, it is appropriate to consider whether LFR should be used to locate these people.

b) Those identified on a case-by-case basis by investigating officers as suitable for inclusion on an LFR Watchlist providing they fall within the criteria at paragraphs 6.8 and/or 6.13 (a)- (f), as applicable.

In these circumstances, the investigating officer (IO) is best placed to assess the need to locate an individual and why LFR is both necessary and proportionate in the circumstances. The IO will also understand what efforts have been made to locate a particular person, or why other options may not be viable in the circumstances. Where an IO decides to pursue use of LFR, they should record their decision and rationale in writing using systems such as CRIS, Crimint, and Merlin. The IO must contact the LFR operational team to have individuals added to the Watchlist using an MPS LFR Form 2 and ensure that they keep their decision to pursue the use of LFR under review. **When an individual no longer needs to be on a Watchlist, the IO must contact the LFR team to have the individual removed with immediate effect**.

6.20 When the AO considers authorising the inclusion of Additional Watchlist Categories, the AO must have regard to the nature of the Deployment when considering Watchlist composition so as to ensure it is not excessive and that the Deployment is one at which there are reasonable grounds to suspect that one or more persons in the Additional Watchlist Category will attend at a time or times at which they are to be sought by means of LFR.

7 MPS LFR Documents

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

(i) Data Protection Impact Assessment* (Review/Amend/Adopt) [8]; *and*
(ii) Equality Impact Assessment* (Review/Amend/Adopt); *and*
(iii) Community Impact Assessment* (carry out); *and*
(iv) The Surveillance Camera Commissioner's Self-Assessment* (Review/Amend/Adopt); *and*
(v) LFR Operational Risk Assessment (carry out).

[8] The DPO and ILSG's roles start during the planning process continue throughout the LFR Deployment – acting as points of contact and providing means of ongoing assurance in relation to data processing queries.

Note: *Any assessment listed above showing `Review/Amend/Adopt' has already been created by the MPS LFR team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each LFR operation. Assessments should remain under continual review to ensure the Deployment falls within them and they remain sufficient for the circumstances as they evolve.

8 Risk Assessment & Resource Levels

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

8.2 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.

8.3 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.

8.4 LFR System Engineers will be deployed to support LFR Deployments and will come with suitable vehicles where required.

8.5 All MPS officers and staff deployed on LFR Deployments must be compliant and in-date with MPS emergency life support (ELS) and officer safety (OST) training requirements. Exceptions to this must be specifically addressed within the written risk assessment. All MPS officers and staff involved in an LFR Deployment must receive LFR training prior to being deployment.

9 Planning & Booking

9.1 As part of the LFR planning process and before the AO authorises a Deployment, the MPS LFR team (including LFR System Engineers) should be consulted on the appropriateness and viability of a Deployment.

10 LFR Operational Roles

LFR Command Team

10.1 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[9])**; 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 and supporting assessments for the Deployment[10]. Gold is to appoint the command team for the Deployment, and to ensure sufficient resources, equipment and personnel will be available to meet their strategic intent for the Deployment. The Gold is to review and adopt the Operational Risk Assessment to ensure that it aligns with their strategic intention for the Deployment.

b) 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.

c) Note: this role is different to the role of MPS SRO for LFR who holds the strategic responsibility for LFR as a capability as opposed to an operational-level responsibility.

d) **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, is responsible for tactical implementation and has front-line responsibility for ensuring compliance with the AO's Authority, the Gold's command and is to monitor the deployment to ensure it stays within the assessments which support the

[9] Note that where the urgency criteria (para 4.4) has been applied, the Gold Commander may be of Inspecting rank. However, this should revert to Superintendent or above as soon as a Superintendent reviews the Deployment and provides authorisation for the Deployment to continue.

[10] Assessments comprise the Data Protection Impact Assessment, the Equality Impact Assessment, the Community Impact Assessment and the Operational Risk Assessment.

Deployment[11]. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having particular regard to the effectiveness of the safeguards in place whilst LFR is being used.

e) **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.

f) **Bronze Community**; Bronze Community is an individual appointed by Silver specifically to oversee and manage community / stakeholder engagement relevant to the LFR Deployment. The Bronze Community should pay particular regard to the Community Impact Assessment.

10.2 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

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

10.4 The LFR Operator should 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 (be it generally or in relation to specific Watchlist images) to the Silver Commander.

10.5 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; *and*

b) what decision was taken regarding whether to Engage a member of the public or not; *and*

[11] Assessments comprise the Data Protection Impact Assessment, the Equality Impact Assessment, the Community Impact Assessment and the Operational Risk Assessment.

c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

LFR Engagement Officer

10.6 LFR Engagement Officers must have an understanding of the LFR system, 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 may be deployed in uniform or plain clothes.

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

10.8 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]. The LFR Engagement Officer should receive an Alert on their handheld device (or otherwise had sight of it) and must then make their own decision about whether they should instigate the Engagement or not. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.

10.9 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.

10.10 Whilst officers must exercise their own discretion when using their powers of arrest and detention, MPS policy is that an LFR system-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.

10.11 If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them

[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. 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.

liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

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

10.13 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 engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so.

LFR System Engineers

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

11 Post-Deployment

11.1 Following each LFR Deployment, the Gold Commander must ensure that a post-Deployment evaluation is completed with a Cancellation Report being produced. 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.

11.2 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.

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

a) total number of individuals <u>*and*</u> the total number of images included in the Watchlist (*there may be multiple images of some individuals*); *and*

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 system was able to generate a Template from them); *and*

c) total number of LFR system-generated Alerts; *and*

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; *and*

f) total number of Alerts that are confirmed as correct (the individual is who the LFR system suggests are); *and*

g) total number of correct Alerts that result in an Engagement that do not require any further police action; *and*

h) outcome of each case where police action is instigated following an Alert; *and*

i) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome.

12 LFR System Security

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

a) images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine; *and*

b) the LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data; *and*

c) the LFR system is physically protected when in use and securely wiped following each Deployment; *and*

d) role based access controls with limited user permissions are implemented on the LFR system; *and*

e) the LFR application is connected to mobile devices using a private access point with three levels of protection; Specific IP addressing, password access to the access point, and password access to the mobile App. The mobile App has a RESTful API and will be covered by SSL; *and*

f) the Dashboard and RESTful API are secured with SSL and TLS by default; *and*

g) all connections are directed through HTTPS; *and*

h) a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*

i) technical issues with the LFR system are always dealt with by LFR System Engineers deployed on the operation.

13 Data Retention & Data Management

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

a) where the LFR system does not generate an Alert, that a person's biometric data is immediately automatically deleted; *and*

b) the data held on 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.

13.2 Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 31 days, except where:-

a) personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*

b) personal data is retained in accordance with the MPS's complaints / conduct investigation policies.

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

a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or*

b) in accordance with the MPS's complaints / conduct investigation policies *and/or*

c) 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 31 days 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.

13.4 To support compliance the LFR system has a full audit capability, and the LFR Operator's log is retained in accordance with MOPI.

13.5 The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether or not protected by encryption, must be reported immediately to the AO, Gold, and the MPS Data Protection Officer.

Register of Deployments

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

a) name and rank of the AO and command team; and

b) date, time, duration, and locality of Deployment; and

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

d) the number of Alerts and the various statistics relating to these; and

e) number of Engagements and their results;

13.7 The MPS will make information relating to LFR Deployments available to the public in accordance with the MPS LFR Documents.

14 Contact Information

14.1 The MPS LFR team can be contacted using the following email address; LFR@met.police.uk.

15 Further Documentation

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

a) Information Management APP; www.app.college.police.uk/app-content/information-managemen t;

b) National Decision Model; www.app.college.police.uk/app-content/national-decision-model ;

c) National Intelligence Management; www.app.college.police.uk/app-content/intelligence-management ;

d) College of Policing Code of Ethics; www.app.college.police.uk/code-of-ethics ;

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