Live Facial Recognition Standard Operating Procedure

INTRODUCTION

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.

The LFR deployments will be delivered using specialist equipment operated by the Hampshire & Isle of Wight Constabulary and Thames Valley Police collaborated Joint Operations Unit, LFR Team. During the preparation and delivery of a specific LFR deployment the LFR Team will be acting under the direction and control of the Chief Constable (as data controller) that is requesting the deployment in their force, according to the arrangements set out in their own LFR Policy and Standard Operating Procedure and other associated LFR impact assessments and documents.

APPLICATION

All Hampshire and Isle of Wight Constabulary (HIOWC) officers and police staff, including the extended police family (including officers from other forces working in support of HIOWC) and those working voluntarily or under contract to the Commissioner should be aware of, and are required to comply with, all relevant HIOWC policy and associated procedures.

This SOP applies in particular to officers and staff 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; 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, LFR Engagement Officer and LFR System Engineers.

Terms and definitions: Capitalised terms used in this LFR SOP shall have the meaning given to them in the HIOWC Police LFR policy document unless otherwise defined in this LFR SOP

Note: This list is not intended to be exhaustive.

TERMINOLOGY

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

AUTHORITY TO DEPLOY LFR

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.

The HIOWC LFR Application / Written Authority Document recognises that the intelligence case for the use of LFR may give rise to a single deployment, within a time-limited period. Where the HIOWC LFR Application / Written Authority Document is to be used to authorise a period of up to 7 days during which the authorised deployments may occur, this provides for a baseline of safeguards to be identified to ensure that the need for the deployment and the currency of the watchlist continues to be maintained daily and with due oversight. Should the need to deploy continue beyond 7 days, the AO will review the original Application / Written Authority Document and consider whether a 7 day extension is necessary and proportionate in the circumstances. Further HIOWC LFR Application / Written Authority Document will be sought. This approach ensures that the use of LFR is time limited but allows an operationally effective way to plan for and deliver LFR as part of wider HIOWC crime-fighting strategies.

Prior to AO authorisation and the deployment of LFR in public spaces, a number of documents must be completed and an HIOWC Chief Officer of NPCC rank[1] must be engaged by the AO. Whilst the Chief Officer does not provide authority for LFR deployment, consultation at this level exists to expose the proposed deployment to an elevated level of strategic thinking, whereby pan-HIOWC issues are taken into account as much as possible. This affords the Chief Officer the opportunity to veto the deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

The Police and Crime Commissioner has been consulted in relation to the use of LFR in principle and the AO must ensure notification is provided to the HIOWC Police & Crime Commissioner (PCC, or designated staff member) prior to any specific deployment.

The authority of the AO:-

a) must articulate the legitimate aim of the deployment and the legal powers that are being relied upon to support the deployment; and

b) means that the AO is satisfied that the deployment complies with HIOWC LFR documents, or is otherwise authorised; and

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

c) must, from a Human Rights Act 1998 perspective, articulate (i) how and why the Deployment is necessary (and not just desirable), (ii) is proportionate to achieve the legitimate aim of the Deployment, and (iii) is in accordance with the law; and

d) must, from a Data Protection Act 2018 perspective, articulate why it is strictly necessary for the HIOWC's law enforcement purposes; meaning that 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; and

   i. Necessary on at least one of the following (or other lawful) grounds (the ground(s) to be confirmed by AO):-
   - Necessary for HIOWC's lawful policing purposes[2] for reasons of substantial public interest; and / or
   - Necessary for the administration of justice; and / or
   - Necessary for the safeguarding of children and/or of individuals at risk; and

   ii. 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 (which may include, in particular, under Articles 2, 5, 9, 10, 11 and 14); and

e) must articulate that the AO has given regard to the safeguards proposed for the deployment and the safeguards contained within the HIOWC LFR documents, and considers based on the information therein 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; and

f) means that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the watchlist complies with HIOWC LFR documents, including the legality, necessity and proportionality criteria; and

g) must articulate any authority to include additional categories of persons to the watchlist, including the legality, necessity and proportionality criteria, in addition to those included to meet the purpose of the deployment; and

h) means that the AO is directing that all police officers / staff engaged in the deployment must have received HIOWC LFR training as per the HIOWC LFR documents (unless they are from another force and they have been trained there); and

[2] This being defined as "is necessary for the exercise of a function conferred on a person by an enactment or rule of law" in the Data Protection Act 2018. This will typically be the ground relied on to support HIOWC Deployments of LFR since this recognises the policing powers conferred on a Constable.

i) means that the AO considers that the deployment is proportionate, with the benefits anticipated from the use of LFR outweighing the concerns and impacts there may be in relation to people's data protection rights, human rights and rights relating to equalities; and

j) means that the AO is satisfied and considers that the control measures in the overarching Data Protection Impact Assessment and Equality Impact Assessment and the deployment specific Community Impact Assessment, are appropriate mitigation measures for the deployment.

k) means the AO has ensured that the minimum Threshold setting to be utilised during the Deployment is aligned with the LFR Policy. The LFR Policy currently stipulates a setting will be equal to or above the value where no FRT System bias is detected (0.64 with the current FRT algorithm).

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.

'WHERE' - DATE, TIME, DURATION AND LOCATION OF DEPLOYMENT

The AO should define the date(s), time(s), location(s) 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

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.

Deployment locations will be determined by there being a likelihood 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.

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; *and*
b) 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.

c) the efficacy of the system with a view to environmental factors to ensure the highest accuracy, along with the ability to ensure effective transparency measures are in place.

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

1. **the reasonable expectations of privacy the general public may have as a whole at that location, this includes the ability to legitimately avoid LFR**:
2. some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy zone in a central city area thoroughfare being typically different to a quiet suburban park or backstreet; and
3. the number of cameras used by the LFR System should also be considered in this context to ensure the size and scale of the deployment enables those on a watchlist to be effectively located without disproportionately processing biometric data; *and*
4. **if a proposed deployment location attracts particular concerns by reference to those expected to be at a particular location**[3]**:**

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.

II. Consideration should be given to available Community Impact Assessment prior to any deployment which is subject to ongoing review during and post deployment.

Where it is practicable to identify a person as 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 and/or wider consultation. Legal advice should be sought where appropriate.

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

[3] 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. This would extend to vulnerable adults. 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.

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

The public should be notified of LFR deployments in advance using force websites and other appropriate communication channels (including social media). It is anticipated that this publicity will then lead to further coverage such as by local news media.

Measures should also be taken during the deployment to ensure the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed. In addition to the use of uniformed officers and marked vehicle(s), other steps for applicants to consider in the context of their proposed deployment location include the requirement for signage placed in advance (outside) of the Zone of Recognition and/or the provision of information leaflets.

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, nor does an attempt to shield one's face from the cameras. HIOWC 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 and in line with policy and training.

Any member of the public who is engaged as part of an LFR deployment must also be offered an information leaflet about the technology. Any person who requires further information relating to LFR will be signposted to the HIOWC LFR operational web page and how to email HIOWC. The LFR web page will provide access to LFR governance documents, privacy notice and appropriate policy document (containing information about data subject's data protection rights) and information about past and future HIOWC LFR deployments.

'WHO' – WATCHLIST GENERATION AND CRITERIA FOR IMAGE INCLUSION ON A WATCHLIST

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

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 HIOWC LFR SOP and be specific

to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a watchlist must comply with the following requirements:-

Requirement	Rationale for the requirement
Intelligence: Watchlists must be driven by a policing need and based on the intelligence case The intelligence case must be current and reviewed before each deployment.	This intelligence-driven approach ensures that the make-up of the watchlist is reflective of, and for the purpose of the LFR deployment
Images sources: Watchlists must only contain images lawfully held by police with consideration also being given as to: • 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 avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: • is of a person intended for inclusion on a given watchlist; and; • is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the watchlist. Regard must be paid to the prospect of the LFR System	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 1:1000 False Alert Rate represents an approach which

Requirement	Rationale for the requirement
generating an alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);	balances these factors in a proportionate way.
Watchlist currency: Watchlists must not be produced, reviewed and imported into the LFR System more than 24 hours prior to the start of the deployment.	This is to ensure the ongoing currency of a watchlist should a deployment be necessarily undertaken for a period of longer than 24 hours.
Watchlist design: Watchlists should benefit from technical measures being adopted through the segregation within the watchlist.	This is to ensure the status of those on a watchlist is recognised by those involved in undertaking engagements in order to ensure the appropriate action is taken should an alert be generated

Additional safeguards relating to protected characteristics

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

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

- There may be different privacy expectations around the use of LFR[4] and that these can be particularly relevant in relation to these people given their potential vulnerability[5].
- HIOWC 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.

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

- aged under 18-years-old;
- aged under 13-years-old;
- a person with a relevant disability[6];
- 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.

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

[4] For example, in relation to 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.

[5] 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)**;

[6] 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[7]	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the watchlist would be using an image of that person taken prior to their reassignment
Safeguards				
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with HIOWC LFR documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images		There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the watchlist.		
Legal Advice		Specific advice must be sought from Legal Services and the HIOWC 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 and make the LFR Operator aware of any such limitations.			
	Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be	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.		

[7] 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.

	blocked from the camera's line of sight.	

Additional Safeguards for Image Quality

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

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

Police-originated images that may be included on a watchlist

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) For the purpose of locating persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison.

b) For the purpose of locating individuals who are designated as a current missing person considered at increased risk of harm that HIOWC has assessed as:

- Medium risk: where the risk of harm to the subject or public is assessed as likely but not serious.
- High risk: where the risk of serious harm to the subject or the public is assessed as very likely.

c) For the purpose of locating individuals shown as outstanding suspects for a range of criminal offences, including high risk crimes and those relating to local district priorities which justifies the inclusion.

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

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 HIOWC or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes, e.g. a missing person considered at increased risk of harm who does not have an existing or viable police-originated image. In these circumstances, consideration may be given to the inclusion of a non-police originated image by the LFR Silver Commander. This will only be used when it is of sufficient quality to allow the LFR system to extract and upload a biometric template and the LFR Operators and Engagement Officers are made aware during a briefing prior to the deployment.

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 source and nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness'. It is recognised that although an image has been made 'public' there is unlikely to be an expectation of it being used to extract biometric data.

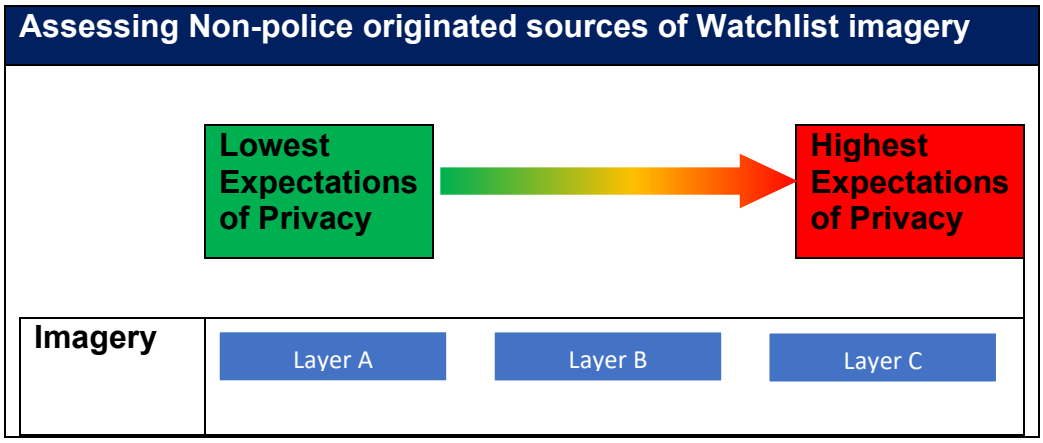

Image Layer	Outline
Non-police originated image – **Layer A**	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images 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 due to their source or nature 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. This would include images obtained by police during non-intrusive covert surveillance.
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 obtain and hold the imagery it has received (for example in the unlikely case of a missing person considered at increased risk of harm where there is no family / friends to provide an image and a confirmed image of the person is obtained from an open source social media site. 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

Image Layer	Outline
	be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.

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 in the paragraph above and that its inclusion is nevertheless proportionate.

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

- Currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison
- Designated as a current missing person and considered at increased risk of harm that HIOWC has assessed as:
    - Medium risk: where the risk of harm to the subject or public is assessed as likely but not serious.
    - High risk: where the risk of serious harm to the subject or the public is assessed as very likely.
- Shown as outstanding suspects for a range of criminal offences, including high risk crimes and those relating to local district priorities which justifies the inclusion.

'Recalled to prison' means that someone who was released from prison on license has breached the conditions of that license. The license to live in the community is revoked meaning that the person must be returned to prison

'Wanted by the courts'. This term includes those with outstanding arrest warrants or who are otherwise required by the courts. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general.

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[8] which the addition to the watchlist addresses;

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

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

HIOWC LFR DOCUMENTS

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); and
ii Equality Impact Assessment* (Review/Amend/Adopt); and
iii Community Impact Assessment* (Create/Adopt); and
iv The Surveillance Camera Commissioner's Self-Assessment* (Review/Amend/Adopt);

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

MANAGEMENT OF RISK & RESOURCE LEVELS

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

The level of trained resources, including back-up contingencies, required to support each deployment is a matter to be determined by the operation's command team. It must be sufficiently resourced to meet transparency obligations.

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 ensures that sufficient resources are available to respond effectively to alerts and to meet the law enforcement purpose of the LFR deployment.

LFR System Operators will be deployed to support LFR deployments where required.

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

Planning & Booking

As part of the LFR planning process and before the AO authorises a deployment, the LFR team (including LFR System Engineers) should be consulted on the appropriateness and viability of a deployment (this team may come from within HIOWC or from another Law Enforcement Agency (LEA)).

LFR OPERATIONAL ROLES

LFR Command Team

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. 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 (Chief Inspector or above); There is only one Silver Commander for any LFR deployment. Silver reports to Gold. Silver has tactical command of the deployment and is responsible for tactical implementation. This officer has absolute authority to suspend or terminate the deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the deployment, having particular regard to the effectiveness of the safeguards in place whilst LFR is being used.
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.

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

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.

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

[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 authority for the Deployment to continue.

LFR Operator must flag any concerns they have regarding LFR System performance to the Silver Commander.

The LFR Operator's log must 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 by the Engagement Officer regarding whether to engage a member of the public or not; and
c) whether an engagement was successfully undertaken, and the outcome of the engagement.

LFR Engagement Officer

LFR Engagement Officers must have an understanding of the LFR application, how it performs, and what effect subject, system, and environmental factors might have.

These officers must receive a full operational briefing prior to deployment. These officers will be deployed in uniform.

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.

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[10]. 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.

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.

Whilst officers must exercise their own discretion when using their powers of arrest and detention, HIOWC 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.

[10] 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.

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

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

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, nor is it an offence in and of itself to seek to conceal one's face while walking through an LFR Zone. 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

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

POST-DEPLOYMENT

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.

The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the deployment and what opportunities exist to improve them for future use, and how learning will be shared.

The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (<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 application was able to generate a Template from them); and
c) total number of LFR application-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 true alert (the individual is who the LFR application suggests are); and
g) total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and
h) total number of correct Alerts that result in an Engagement that do not require any further police action; and
i) outcome of each case where police action is instigated following an Alert; and
j) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome; and
k) Threshold setting for the Deployment

LFR APPLICATION SECURITY

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

a) The watchlist will be downloaded from HIOWC crime recording systems onto an encrypted USB. The watchlist will be uploaded onto the standalone LFR system from the encrypted USB, on HIOWC Police premises. The LFR Silver Commander will be accountable for the safe keeping and eventual daily deletion of watchlist images from the encrypted USB.
b) the LFR application is a fully-closed system with two layers of password protection to access the application; and
c) the LFR application is physically protected when in use and deployment data stored on the system is securely wiped following each deployment; and
d) role based access controls with limited user permissions are implemented on the LFR application; and
e) the LFR application can be 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.
f) the dashboard and RESTful API are secured with SSL and TLS by default; and all connections are directed through HTTPS; and
g) a full audit is maintained of all user initiated actions undertaken during the course of a deployment; and
h) technical issues with the LFR application are always dealt with by LFR System Engineers deployed on the operation.

DATA RETENTION & DATA MANAGEMENT

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

a) where the LFR application does not generate an Alert, that 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.

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

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

a) due to its relevance in a criminal investigation and is held in accordance with the Data Protection Act 2018, the UK GDPR (if applicable) MOPI and the Criminal Procedures and Investigations Act 1996; and /or
b) in accordance with the HIOWC's complaints / conduct investigation policies.

To support compliance the LFR application has an audit capability.

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 HIOWC Data Protection Officer.

Register of Deployments

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;

The HIOWC will make information relating to LFR deployments available to the public in accordance with the HIOWC LFR documents.

FURTHER DOCUMENTATION

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

a) Information Management APP; www.app.college.police.uk/appcontent/information-management
b) National Decision Model; www.app.college.police.uk/app-content/nationaldecision-model
c) National Intelligence Management; www.app.college.police.uk/appcontent/intelligence-management
d) College of Policing Code of Ethics; www.app.college.police.uk/code-ofethics
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); www.judiciary.uk/wpcontent/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

g) Court of Appeal Ruling - R (On the application of Edward BRIDGES) v (1) The Chief Constable of South Wales Police and (2) The Secretary of State for the Home Department and others [2020] EWCA Civ 1058:
h) Facial Recognition APP
i) Surveillance Camera Commissioner's guidance:
j) Information Commissioner's guidance.