HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

STANDARD OPERATING PROCEDURE

Live Facial Recognition

Document Type:	**Standard Operating Procedure**
SOP Owner:	**Assistant Chief Constable – Operations**
Department:	**Operational Support Services**
SOP Writer:	**Sergeant Joseph Dunn**
Version:	**1.1**
Effective Date:	**08.04.24**
Recommended Review Date:	

Version No	Date	Author	Changes
1.0	07.03.24	Sergeant Joseph Dunn	Initial writing
1.0	29.4.24	Sergeant Joseph Dunn	Changes made following policy consultation

CONTENTS

1. INTRODUCTION

Live Facial Recognition (LFR) is used by North Wales Police (NWP) as an overt, precision crime-fighting tactic to locate people who are wanted for criminal offences, or those in breach of, or attempting to breach lawfully imposed conditions.

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist, to locate persons of interest by generating an alert when a possible match is found. Police officers on the ground then approach and interact with persons subject to an alert, and take any policing action as necessary.

LFR technology is not owned or operated by North Wales Police. It will be brought to the force area on Mutual Aid for specific deployments, and it will be operated and staffed by specialist

trained operators from the supplying force, supported by NWP assets. NWP will be responsible however for the deployment and the use of LFR within the NWP force area.

The APP in regard to LFR should be adhered to at all times and this standard operating procedure is not a substitution for APP.

NWP Policy on the use of LFR should also be taken into account.

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.

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;

c) All Authorising Officers (AO);

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

e) LFR Operators, LFR Engagement Officer and LFR System Engineers.

Note: This list is not intended to be exhaustive.

This SOP focusses exclusively on LFR. Terminology relating to LFR is defined within the NWP LFR policy document, and also within the APP for this area of business - Terminology | College of Policing

2. Authority to deploy LFR

LFR may be deployed in NWP on mutual aid from other forces who host the capability to support a dedicated policing operation, or in response to intelligence / operational need. The LFR equipment and operators will be provided by the supporting force, but under the direction, control, and support of NWP resources.

The officer applying for the use of LFR must make contact with the NPCC Staff Office. Any proposal to bid for LFR on Mutual Aid must be agreed by the NPCC Team.

The Staff Office will then speak with, or facilitate contact with, the force supplying mutual aid (currently SWP) and the viability and logistics of a proposed deployment must be discussed with the providing force.

If the proposal for a deployment is provisionally agreed, then an officer of not below the rank of Inspector must complete the LFR application, and in normal circumstances, the authority to deploy LFR in support of a policing operation should be made by an officer not below the rank of Assistant Chief Constable. Their authorisation to do so should be recorded in writing, on the dedicated NWP authorisation form.

Once completed, a copy of the Application and the Authority, along with supporting documentation will be sent to the force providing the LFR technology for authorisation of deployment on mutual aid.

The mutual aid requirement will then be processed as usual through the National Police Operations Co-ordination Centre (NpoCC) and the relevant Regional Information and Control Centre (RICC) via Ops Planning.

The AO's written authority provides a decision making audit trail demonstrating how the AO has considered the legality, necessity and proportionality of the deployment, the safeguards that apply to the deployment and the alternatives that were considered but deemed to be less viable to achieve the policing purpose.

The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR deployment.

The written approval will be retained in accordance with MOPI, APP, and other relevant legislation or policy and be made available for independent inspection and review as required.

The NWP LFR application / written authority document recognises that the intelligence case for the use of LFR may give rise to a single deployment, or a need for a series of deployments within a time-limited period. Where the NWP LFR application / written authority document is to be used to authorise a period of up to 7 days during which deployments may occur, the form provides for a baseline of safeguards to ensure that the need for the deployment and the current nature of the watchlist continues to be maintained with due oversight.

Should the need to deploy continue beyond 7 days, a further application / written authority is required.

This ensures that the use of LFR is time limited, yet still allows an operationally effective way to plan for and deliver LFR in support of the aims and objectives of North Wales Police.

The authority of the AO must include the following:

a) An articulation of the legitimate aim of the deployment, and the legal powers relied upon to support it

b) Confirmation that the AO is satisfied that the deployment complies with this policy and APP

c) Confirmation that from a Human Rights Act 1998 perspective the deployment is necessary (not just desirable), and that it is a proportionate means to achieve the legitimate aim of the deployment

d) Regarding the Data Protection Act 2018, articulate that the authority to deploy is strictly necessary for NWP's law enforcement purposes – therefore that there is a 'pressing social need', and it is not reasonably viable to address this through less intrusive means, either because less intrusive tactics have been tried, or it is believed that those tactics are unlikely to be effective,

i. Regarding the Data Protection Act 2018, that the deployment is necessary[1] on at least one of the following grounds: For a lawful policing purpose regarding reasons of substantial public interest
ii. Necessary for the administration of justice
iii. necessary for the safeguarding of children and/or of individuals at risk

e) must articulate that the AO has given regard to the safeguards proposed for the deployed, and the safeguards contained within NWP LFR documents, and that they consider 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 1988, the Data Protection Act 2018 and GDPR

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

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,

h) confirmation 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 human rights and rights relating to equalities,

i) confirmation that the AO is satisfied that the control measures in the Data Protection Impact Assessment, Community Impact Assessment (if in place), and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the deployment.

j) confirmation that the AO has determined the minimum threshold setting to be utilised during the deployment. Ordinarily this setting will be equal to or above the value where no Facial Recognition Technology (FRT) system bias is detected (0.64 with the current FRT algorithm used). The threshold value may be lowered based on the intelligence case, with a full rationale detailed in the application / written authority document.

The AO must notify the office of the Police and Crime Commissioner prior to any deployment.

3. 'Where' - Considerations for date, time, duration and location of the deployment

The authorisation for LFR deployment should define the date, time, location, and duration that 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

[1] 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 NWP Deployments of LFR since this recognises the policing powers conferred on a Constable.

The potential deployment location will be substantially informed by the intelligence case, the policing purpose to include a person on a watchlist, any community impact assessment, and environmental factors.

Deployment locations will be selected by there being reasonable grounds to suspect that the proposed deployment location is one where persons on the watchlist will be present at a time, or times, during which the deployment is active and at a time they are 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 should be further supported by:

a) policing information or intelligence about a proposed deployment location, including if there is an increased risk to public safety, 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.

When reviewing a potential deployment location, consideration must be given to those who are likely to pass the LFR cameras, and also to:

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

b) the number of cameras used by the LFR system should be considered in this context, to ensure that the size and scale of the deployment enables those persons on a watchlist to be effectively located without disproportionately processing biometric data, and,

c) whether the proposed deployment location is likely to attract particular concerns due to those expected to be at a particular location – such as hospitals, places of worship, centres for legal advice, polling stations, schools (and other places frequented by children), care homes, and locations where persons are attending a lawful assembly or demonstration are (as they may feel less able to express their views, or otherwise be more reluctant to be in the area).

Locations of particular concern / greater expectation of privacy

If a deployment location is likely to attract particular concerns / raise issues of a greater expectation of privacy, then significant strategic considerations should be documented and any potential issues mitigated, as much as possible, within the written authority.

This could include liaising with a person responsible for the location / demonstration / assembly as part of a community impact assessment, explaining the legitimate policing aims and why LFR is considered necessary, and obtaining legal advice specific to the deployment.

In these circumstances, the AO must consider the necessity to deploy LFR to that particular location, and whether the aims of the operation could be similarly achieved by deploying to a different location.

If it is deemed necessary to deploy in that specific location, with the processing of biometric data being strictly necessary, then within their strategic considerations, and alongside considering mitigations, the AO needs to weigh the rights of those engaged by the LFR system against the likely benefits of it.

This is to ensure that the policing action proposed is not disproportionate to the aim being pursued.

Cameras and Camera Placement

The providing force on Mutual Aid will be responsible for providing the appropriate equipment, however it should adhere to the following guidance to ensure the best chance of success.

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

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

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

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

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

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

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

4. 'How' - Measures during an LFR deployment

Save in exceptional operational circumstances where doing so would undermine the objectives of the deployment, the public should be notified of LFR deployments in advance, using the force public website, and other appropriate communication channels.

By being open and transparent around our use of LFR, and where appropriate, the policing objectives aiming to be achieved by LFR, we seek to maintain public trust and confidence, and ensure that the public are not engaged by LFR technology without prior warning.

To this end, measures should be taken during the deployment to ensure that the policing presence is overt, and that allow the public to establish that LFR is being used, and to understand the nature of the data being processed.

Measures which should be used to achieve this are, but not limited to:

a) the use of uniformed officers and marked vehicles

b) the use of signage placed outside the Zone of Recognition advising of the use of LFR

c) leaflets providing information / a link to the force website where information on LFR and answers to frequently asked questions can be found.

In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any deployment is overt, the objectives for the deployment and its use as policing tactic will also be relevant if the policing need to deploy is to be realised.

For example, unduly extensive signage may undermine the effectiveness of a deployment seeking to locate persistently outstanding offenders. By comparison a deployment seeking to protect a site, or a particular event may merit multiple levels of signs and the proactive distribution of leaflets as a deterrent.

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. NWP staff deployed to a an operation using LFR must be accountable for their own actions, and must exercise any powers in accordance with the NDM, within legal framework, and with regard to the Code of Ethics.

Any member of the public engaged with as part of an LFR deployment should, unless it is impracticable to do so due to operational reasons, be offered an information leaflet which provides details about the LFR technology used.

All information materials, such as signage, leaflets, website and social media communication must be bilingual, in Welsh and English.

Any person who requires further information relating to NWP's use of LFR should be provided with the group email address of LFR@northwales.police.uk.

5. '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 NWP 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 in question
Image 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 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	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 NWP SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way. This False Alert Rate is also in keeping with APP.

Requirement	Rationale for the requirement
adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);	
Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the deployment.	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 legal challenges in relation to the use of LFR, and specifically the ruling within Bridges V Chief Constable of South Wales Police (2020), in December 2020 the then Surveillance Camera Commissioner (SCC)fa published a 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. NWP have considered best practice with regard to LFR, and any controls, mitigations and processes contained within this SOP reflect the LFR system's performance and NWP's specific criteria for deployment of LFR and inclusion of persons within a Watchlist.

NWP has confidence in the LFR system's performance, particularly in relation to gender, age and race, and that the use of LFR does not amount to unlawful discrimination.

However, it is recognised that regardless of the performance considerations, NWP should take particular care when considering and publishing details regarding a deployment, and specific characteristics relating to those identified, with regard to:

1) Age – including the protection of children, particularly the very young

2) Persons with a disability

3) persons who have and/or are undertaking a gender reassignment.

This is because:

1) there may be different privacy expectations around the use of LFR[2], and these can be particularly relevant in relation to the above groups given their potential vulnerability[3]

2) those who may be involved in criminality have the capability and capacity 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.

Within NWP, regarding each deployment of LFR, it must be specifically identified and documented if the watchlist contains persons who are believed or suspected to be:

a) aged under 18

b) aged under 13

c) a person with a relevant disability [4]

e) a person who has undertaken a gender reassignment and it is believed or suspected to be the case that the Watchlist would be using an image of that person taken prior to such reassignment.

On the next page, a chart is displayed which outlines further, specific safeguards that apply to the composition of the Watchlist.

[2] 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.

[3] 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)**

[4] 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 aged 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 13 and that person's records state that person is aged (or suspected to be aged) under 13-years-old[5]	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 the case 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 NWP LFR SOP, 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 NWP LFR team prior to seeking authorisation from the AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		
Technical Advice	Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.			
	Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be blocked from the camera's line of sight.	Technical advice should be sought on a case-by-case basis to inform this assessment, which will be directed to the LFR team within the force supplying the LFR technology on mutual aid. 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.		

[5] Generally, studies [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

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 an offence, 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 graded at medium or high risk; and/or

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

f) victims of an offence, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progression of an investigation, or is otherwise a close associate of an individual who would fall within criteria (a) – (e).

A rationale for each is as follows:

a - 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.

b - Suspected of having committed, be about to, or to be committing an offence. This encapsulates persons who are wanted by the police pre-charge in relation to them being suspects for an offence. This falls within the common law purpose of the police to investigate, prevent and detect crime.

c – Bail conditions, court order, or other restrictions that would be breached. This takes into consideration the fact that an assessment has already been made by either the police or the courts to impose conditions, usually for safeguarding or preventative reasons, and that it is again within the common law purpose of the police to prevent and detect any such breaches.

d – Missing persons graded at medium or high risk. MFH cases of medium or high risk mean that the subject is at risk of danger to themselves or others, with high risk reserved for cases of an immediate risk with substantial grounds for believing that the subject is in danger, or that the public is in danger. Both categories engage the police's responsibilities

under Article 2 of the Human Rights Act, and the use of LFR to locate the person is a proportionate way of doing so given the risk and the obligations under Article 2.

e - Presenting a risk of harm. Mitigating the risk of harm to themselves or to others 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, perhaps because of fraud or other dishonesty. It can also include 'harm' in the context of posing a risk to national security.

The risk of harm will be informed by the intelligence case and/or the considerations set out in the applicable LFR deployment application form. This will need to inform the AO as to how the individual or group of individuals present(s) a risk of harm to themselves or to others and:

a) how using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*
b) why the significance of the harm identified means it is **necessary** for the police to take action in order to manage the risk.

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

f - victims of an offence, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progression of an investigation, or is otherwise a close associate of an individual who falls under one of the previous headings. This criteria includes a victim, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progress of an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within one of the aforementioned categories that may be deemed appropriate for inclusion within an LFR Watchlist.

The threshold for any Watchlist inclusion is high and the use of this category will be by exception with regard to strict critera. 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 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

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) 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.

Non-custody images

Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed, which includes case by case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a watchlist to meet a policing objective, and the proportionality of using such images on an LFR system.

Non-police originated images that may be included on a Watchlist

As a general rule, suitable police originated images should be preferred for inclusion on a Watchlist. However, there will be occasions where no image is held by NWP or the wider law enforcement community to allow inclusion of a specific person on a Watchlist, or if an image is held by law enforcement, then its quality is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.

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’ which are described below.

Assessing non-police originated sources of Watchlist imagery

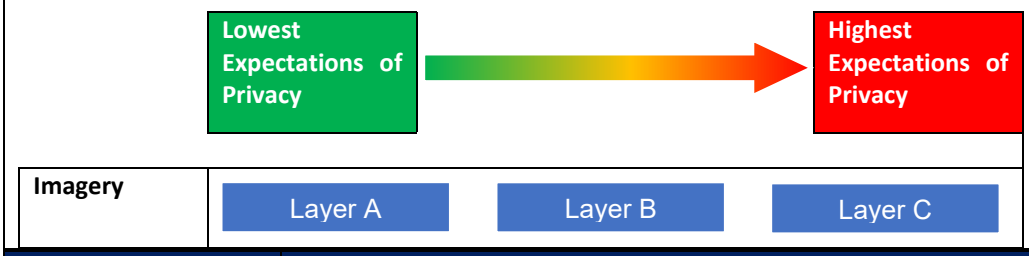

Image Layer	Outline
Non-police originated image – **Layer A**	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images 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 they have been 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.

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 relating to the image and in particular which layer of intrusiveness the image is attributable to and the factors within the above table.

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 an offence, or where there are reasonable grounds to suspect that the individual is about to commit 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 at high or medium 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 one of the above criteria.

6. Management of risk and resource levels

Each deployment should be risk assessed in line with NWP procedure, in the planning stage and within the operational order. 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 resources, including back-up contingencies required to support each deployment is a matter to be determined by the operation's command team.

Currently NWP will obtain LFR technology on mutual aid from South Wales Police (SWP).

SWP will provide the technology, operators, a supervisor and an Inspector to oversee the use of the LFR technology. NWP will be responsible for providing sufficient resources to engage with members of the public subject to an LFR Alert, to arrest if necessary and convey to custody, and to provide sufficient staffing to allow an effective deployment.

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, to engage with the public, and to meet the law enforcement purpose of the LFR deployment. **If the engagement teams are depleted, then the use of LFR will cease until sufficient resources are available.**

For specific advice and guidance on resource levels and staffing required for engagement, the force providing the LFR technology on mutual aid must be consulted with. As a general guide however, it should be planned for at least two persons to be assigned to each LFR camera.

All NWP officers and staff deployed on LFR deployments must be in date with NWP First Aid and officer safety training requirements.

The force providing mutual aid will be responsible for ensuring their staff are compliant and in date with their First Aid and Safety Training policy, and that they have received LFR training prior to being deployed on mutual aid to NWP.

7. Planning and booking

As part of the LFR planning process and before the AO authorises a deployment, the SWP LFR team – as the force currently supplying mutual aid – should be consulted with on the appropriateness and viability of the proposed deployment. This can be facilitated via the NPCC Staff Office by contacting a.staffofficers@northwales.police.uk

Early consultation with the NPCC team is advised prior to any consideration for LFR deployment.

8. LFR operational roles

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 – Chief Superintendent or above**. There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their strategic intention aligns with the Authorising Officer's 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 if they are of at least the rank of ACC.

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 absorbed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

LFR Operator

LFR Operators will be provided and deployed by the force on mutual aid. They 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 LFR Operator must flag any concerns they have regarding LFR system performance to the Silver Commander.

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

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 may be deployed in uniform or plain clothes.

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 involved in 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 one

should take place. 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. Any officer must form their own `reasonable grounds for suspicion' (which may rely on information provided by others, for example the LFR technology / Operator), and/or have a clear understanding of the legal basis supporting any action they take.

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, it is NWP's SOP 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.

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. 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 for the use of any other policing power where it is right and proper to do so.

9. 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 (including what methods were used to obtain them):-

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

10. LFR Application Security

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

a) images are transferred onto the LFR application via an encrypted USB device or via a secure connection to the SWP Virtual Private Network (SWP being the force NWP are using to supply LFR technology) ; and

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. 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 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

11. Data Retention & Data Management

North Wales Police must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the NWP LFR documents, data protection legislation and the APP on the use of LFR.

This means that:-
a) where the LFR application 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.

c) Where the LFR application generates an Alert, all personal 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) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or

b) in accordance with the NWP's complaints / conduct investigation policies.

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

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 NWP 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;

NWP will make information relating to LFR Deployments available to the public in accordance with guidance contained within NWP policy on the use of LFR.

12. Contact Information

For information on this Standard Operating Procedure, please contact a.staffofficers@northwales.police.uk

13. Supporting documentation

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

- DPIA
- Equality Impact Assessment
- Community Impact Assessment
- Appropriate Policy Document