



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date:05/12/2025

2025/1233 - Facial Recognition Technology [FRT]

In response to your recent request for information regarding;

I seek information on the use of live and retrospective Facial Recognition Technology [FRT] in policing large public events, and especially football matches.

We hereby request access to the following information:

1. How often has live FRT been deployed on police vehicles outside of football matches since 11 August 2023?

Information is available on our website;

[Live Facial Recognition | North Wales Police](#)

1.1. How does the police department determine whether live FRT will be deployed?

See attached policy and operating procedure

1.2. Do police provide advance notice to ticket holders and football clubs before live FRT is deployed?

See attached policy and operating procedure for information on advance notice

2. How many arrests have been made following the use of live FRT when deployed outside of football matches, or retrospective FRT when deployed at or outside football matches, since the football season starting 11 August 2023?

See updates [Live Facial Recognition | North Wales Police](#)

2.1 How many such arrests (i.e., arrests made as a result of live or retrospective FRT) led to the issuance of a football banning order?

Not applicable

3. When issuing new football banning orders, do police consider information from football clubs?

No information held in this office about the issuing of banning orders

3. When monitoring outside of football matches with live FRT, do police share images of people identified with live FRT with football clubs?

See policy and S.O.P for information

5. Are people with active or expired banning orders added to a database used in conjunction with live or retrospective FRT when deployed for other law enforcement purposes?

See policy and S.O.P for information on watchlist compilation

5.1 In particular, are such people added to a database used for live or retrospective FRT at any other public events?

As above

6. Have there been any incidents of misidentification as a result of FRT deployed outside of public events since 2023?

See updates [Live Facial Recognition | North Wales Police](#)

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 04/12/2025



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Live Facial Recognition

Governance:			
Document Type:	Policy		
Policy Owner:	ACC Operations		
Department:	NPCC		
Policy Writer:	Sergeant Joseph Dunn		
Policy Number:		Version:	1.0
Effective Date:			
Recommended Review Date:			

POLICY

CHANGE HISTORY				
Version No	Author	Changes	Ratification	Date
1.0	Sgt Joseph Dunn	Initial draft		5.4.24
1.1	Sgt Joseph Dunn	Changes made following governance review		29.4.24

CONTENTS

1. WHY IS THIS POLICY REQUIRED?	2
2. WHO SHOULD USE THIS POLICY?	3
3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?	3
4. Terminology	3
5. LFR Overview.....	8
6. Strategic Intention, Objectives and Use Case.....	10
7. The LFR Deployment Process.....	12
8. Governance, Oversight and Impact Assessments	14
9. Oversight Bodies and Regulatory Framework.....	18
10. Public Engagement	19
11. Watchlist Considerations	20
12. Testing Equitability	23
13. Design Guidelines for LFR	24
14. Cameras and Camera Placement	25
15. Key Performance Metrics	26
16. LFR Guidance Summary.....	Error! Bookmark not defined.
17. Acronyms used in LFR	27

1. WHY IS THIS POLICY REQUIRED?

1.1 Live Facial Recognition (LFR) is used by North Wales Police as a precision crime-fighting tactic to locate people who are wanted for criminal offences and helps protect the most vulnerable in our society. More detail about how LFR works and how NWP uses it can be found in section 5 (LFR Overview).

1.2 The APP on LFR details that each force should develop an overarching policy document that details our force's approach to using LFR, with a commitment to using overt LFR technology in a responsible, transparent, fair and ethical way, in accordance with all relevant law and only when other, less intrusive methods would not viably achieve the legitimate and lawful policing objectives. Whilst this policy, and associated guidance should be read in conjunction with APP, as LFR is a national tool, this policy has been created to adhere to the national guidance contained within the APP.

1.3 This policy aims to: -

a) provide NWP personnel and members of the public with information about NWP's present strategic, operational and technology objectives for the overt use of LFR, such that it enables NWP to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives); and

b) provide NWP personnel with guidance on the Deployment of overt LFR technology by NWP in spaces accessible to the public to meet NWP's objectives for LFR; and

c) establish the governance structure for the Deployment of LFR, ensuring that NWP use of LFR is appropriately governed and legally compliant; and

d) provide an overview of LFR technology and advise on practical issues such as camera selection and placement in order to obtain the best performance from the LFR system.

1.4 Not in Scope

There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR), which relates to non-real-time searching of images against a database. Also, not in scope is Operator Initiated Facial Recognition (OIFR) where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis.

In summary, this guidance does not extend to:-

a) manually instigated facial recognition for retrospective searching of video / still images; or

b) human initiated facial search submitted from a mobile device in near real-time; or

c) any NWP use of third-party LFR systems, or data sharing for the purpose of facilitating the use of those systems. In such instances additional privacy

considerations would be required (e.g. additional Information Sharing Agreements and audit requirements), which are beyond the scope of this guidance; or

d) the legal framework that is applicable to NWP's use of LFR – this is separately detailed within NWP's Legal Mandate document.

2. WHO SHOULD USE THIS POLICY?

- 2.1 This policy should be used by persons considering the deployment of LFR, commanders in LFR deployments, those involved in the planning, application and implementation of LFR deployments, and staff involved in LFR deployments.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

- 3.1 This policy should be read in conjunction with the APP provided by the College of Policing on Live Facial Recognition.
- 3.2 A number of documents are available to supplement this guidance and these include but are not limited to, the:-
- a) NWP LFR Standard Operating Procedure (SOP)
 - b) NWP LFR Data Protection Impact Assessment (DPIA)
 - c) NWP LFR Legal Mandate
 - d) NWP LFR Appropriate Policy Documents
 - e) NWP LFR Equality Impact Assessment Screening

4. Terminology

- 4.1 Within NWP and throughout NWP LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition:-

Adjudication

A human assessment of an alert generated by the Live Facial Recognition (LFR) application by an LFR engagement officer (supported, as needed by the LFR operator) to decide whether to engage further with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject, system and environmental factors.

Administrator

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

Alerts

An alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the watchlist and returns a comparison (similarity) score above the threshold.

True Alert

A true alert is determined when the probe image is the same as the candidate image in the watchlist.

Confirmed True Alert

Following engagement, a confirmed true alert is determined when the engaged individual is the same as the person in the candidate image in the watchlist.

True Recognition Rate

It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated).

This is also referred to as the true positive identification rate.

False Alert

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement. (The false alert rate is one of the two measures relevant to determining application accuracy).

Confirmed False Alert

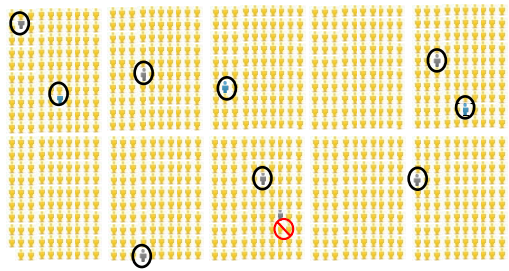
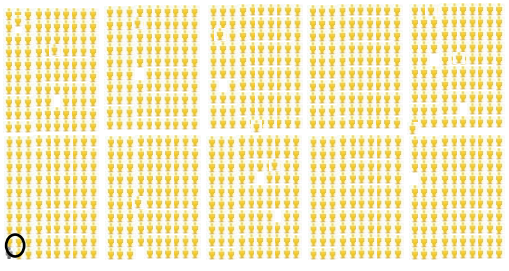
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

False Alert Rate

The number of individuals that are not on the watchlist who generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition. This is also referred to as false positive identification rate.

Application Accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the True Recognition Rate and the False Alert Rate. This is further explained on the following page. The example given has been simplified to demonstrate the concept, but note that the metrics have been calculated in accordance with the agreed scientific method as set out by the International Organisation for Standardisation:

True Recognition Rate		False Alert Rate
What is it?	It is the total number of times an individual(s) on a watchlist known to have passed through the Zone of Recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the Zone of Recognition. This is regardless of whether an alert is generated by the LFR application or not.	Is the number of individuals that are not on the watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
Worked Example	 The True Recognition Rate would be 90% if 10 people on the watchlist each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people (with no alert being generated against the 10th person).	The False Alert Rate would be 0.1%, if for every 1,000 people that passed the LFR system, an Alert was generated against one person who was not on the watchlist. 

Authorising Officer (AO)

The officer (usually holds the rank of Superintendent or above according to APP, but within NWP the AO is of the rank of ACC or above) who provides the authority for LFR to be used.

Biometric Template

A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

Blue Watchlist

A watchlist comprises known persons that can be used to test system performance, for example, police officers / staff may be placed on a blue watchlist and 'seeded' into the crowd who walk through the zone of recognition during a deployment.

Candidate Image

Image of a person from the watchlist returned as a result of an alert.

Deployment

Use of an LFR application as authorised, as authorised by an AO to locate those on an LFR watchlist.

Deployment record

An amalgam of the LFR application, the written authority document and the LFR cancellation report. This sets out the details of a proposed deployment including – but not limited to:

- a. location
- b. dates and times
- c. deployment and watchlist rationale
- d. legal basis
- e. necessity
- f. proportionality
- g. safeguards
- h. watchlist composition
- i. authorising officer
- j. resources
- k. relevant statistics
- l. outcomes
- m. summary of any issues
- n. threshold setting

Engagement

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

Environmental Factors

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

Faces per frame

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

Facial Recognition Technology (FRT)

This technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database and generates possible matches. This is based on digital images (either still or from live camera feeds).

False Negative

Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are a number of reasons false negatives occur; these include application, subject and environmental factors, and how high the threshold is set.

Gold Commander

Is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment. (They are responsible and accountable for the policing operation/event and determine the strategic objectives).

Live Facial Recognition (LFR)

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist in order to locate persons of interest by generating an alert when a possible match is found.

LFR Engagement Officer

An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR deployment.

LFR Operator

An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

LFR System Engineer

A person who NWP deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of an LFR system.

Person(s) of Interest

A person on a watchlist

Possible Match

A person returned as a result of the probe and candidate image being of sufficient similarity above the threshold.

Probe Image

A facial image which is searched against a watchlist.

Recognition Time

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

Retrospective Facial Recognition (RFR)

A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.

Silver Commander

The officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander. (The silver commander develops, commands and coordinates the overall tactical response of an operation, in accordance with the strategic objectives set by the gold commander).

Similarity Score

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

Subject Factor

A factor linked to the individual, for example, demographic factors or physical features or behaviours for example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.

System Factor

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

Threshold

The configurable point at which two images being compared will result in an alert. The threshold needs to be set with care to maximise the probability of returning true alerts whilst keeping the false alert rate to an acceptable level.

Urgency

In the context of authorising an LFR deployment, a deployment that is related to an: Imminent threat-to-life or serious harm situation; and/or intelligence / investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action.

Watchlist

A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (from the reference image database) and will have been created specifically for the LFR deployment.

Zone of Recognition

A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.

5. LFR Overview

- 5.1 Live Facial Recognition (LFR) is used by NWP as a precision crime-fighting tactic to locate people who are wanted by NWP and/or the Courts. It helps us protect the most vulnerable in our community.
- 5.2 LFR also helps us locate those on a Watchlist, by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist of Candidate Images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. Watchlists composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment.
- 5.3 LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify Possible Matches against persons of interest to Law Enforcement

Agencies. Where the LFR application identifies a Possible Match, the LFR system flags an Alert to a trained member of personnel who then makes a decision as to whether any further action is required. In this way, the LFR application works to assist NWP personnel to make identifications rather than acting as an autonomous machine based process devoid of user input.

LFR and North Wales Police

- 5.4 NWP uses LFR technology supplied by South Wales Police (SWP). This is on a mutual aid basis, where the technology is operated by SWP, but under the authority, direction and control of NWP.
- 5.5 LFR has been trialled by SWP over a period of six years. Whilst NWP is its own law enforcement entity, we are aware of the results of these trials, and NWP believes that LFR is a valuable precision policing tool that can assist NWP to keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.
- 5.6 The following are illustrative examples where LFR may assist NWP with its policing purposes:-
- a) Supporting the location and arrest of people wanted for criminal offences;
 - b) Preventing people who may cause harm from entering an area (e.g. under football banning orders);
 - c) Supporting the identification of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons, sex offenders etc.);
 - d) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.
- 5.7 Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. NWP is conscious that the use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.
- 5.8 It is therefore incumbent on NWP to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR.
- 5.9 As the use of LFR by SWP has been in place for a number of years, and in seeking to address other potential concerns, SWP has facilitated academic research led by the National Physics Laboratory, and has proactively engaged with civil liberty interest groups. SWP has also commissioned the National Physical Laboratory (NPL) to undertake a ground-breaking equitability study on the use of LFR technology in an operational context to further build on the high levels of diligence already conducted on the FRT algorithm. NWP is grateful to SWP for undertaking this work, which seeks

to reassure our communities. The results of this research can be found on the SWP website.

- 5.10 Whilst it is important to note that North Wales Police has its own identity, we have taken the key learning and development of this policing tool, conducted by South Wales Police, and have used this to formulate our approach. As part of their development of the use of LFR, SWP has listened carefully to many parties with an interest in the use of LFR and has carefully considered what safeguards are necessary to support the use of LFR. NWP recognises this work, and our protocols mirror those of SWP, to ensure that we are putting in place adequate safeguards in line with best practice.
- 5.11 Each deployment must be carefully designed and have clear documented objectives.
- 5.12 The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality.
- 5.13 Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any concerns the public may have with regards to how their human rights are engaged.
- 5.14 The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the Deployment are appropriately trained, briefed, and accountable. Also, that equipment will be used correctly, and that those involved in the deployment mitigate against inappropriate responses to LFR application Alerts.
- 5.15 The AO must also consider how the Deployment of LFR may impact on communities as a whole, and how the rights of everyone whose image is likely to be captured by the LFR application have been considered, and what safeguards are in place to protect them.
- 5.16 NWP is not only concerned with developing and implementing precision policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. NWP will implement a robust governance process to review the effectiveness and impact of LFR deployments on an ongoing basis. NWP will focus on delivering transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from North Wales communities as part of an ongoing process.
- 5.17 This guidance document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

6. Strategic Intention, Objectives and Use Case

- 6.1 LFR Deployments must be run under a Written Authority Document that complies with the following strategic intentions and operational objectives.

6.2 Strategic Intentions

NWP will:-

- a) use overt LFR technology in a responsible way to locate offenders in accordance with NWP's common law policing powers. This includes targeting those wanted for criminal offences, those who pose a risk of harm and those wanted by the courts.
- b) comply with the common law and statutory safeguards in delivering its policing operational duties, and relies on the common law to discharge a number of its duties. LFR can assist with NWP's duties to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security. This includes targeting those wanted for offences. It also includes using LFR technology to protect the public, reduce crime and help safeguard vulnerable persons.
- c) strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to make North Wales the safest place to live, visit and work in the U.K
- d) build public trust and confidence in the development, management and use of LFR by taking account of privacy concerns and maximising transparency; and
- e) maintain good governance through a command structure that incorporates strategic, operational and technical leads for the deployment of LFR, with clear decision making and accountability; and
- f) ensure that the deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and NWP LFR Documents; and
- g) transparently identify, manage and mitigate reputational and organisational risk to NWP; and
- h) be recognised as a progressive, responsible and ethical organisation.
- i) NWP will ensure that LFR is used ethically in order to protect the tactic from reputational harm for national policing.

6.3 Operational Objectives

NWP will:-

- a) use LFR technology to enable NWP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities; and
- b) adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight is active and involved, with the officer retaining full control and making the decision on whether or not to take action; and
- c) engage with and provide reassurance to communities, listening and responding to concerns; and
- d) continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

6.4 Technological Objectives

6.5 NWP will:-

- a) ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and
- b) ensure that the force providing the technology provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other imprisonable offences; and
- c) look to technological improvements whilst keeping the NWP LFR SOP under review. Where appropriate we will trial alternative providers of facial recognition software and hardware in parallel with our current provision of using SWP assets. This helps to ensure that the best possible service is sought, and we are able to proactively develop improved working methodologies and accuracy. The outcomes of any parallel trial will be captured with the same key performance metrics that are gathered when deploying LFR to ensure the findings are suitable for direct comparison and analysis. All detailed retention periods will remain unaffected.

6.6 Use of LFR

- 6.7 This guidance relates to the use of LFR in an overt capacity to help NWP protect the public. NWP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool.
- 6.8 LFR helps NWP use its resources more efficiently. NWP considers that LFR is better than humans at recognising persons from a large dataset (generally hundreds to low thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to NWP.
- 6.9 The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies. (It is acknowledged that considerations regarding data protection should not be considered as an absolute barrier to information sharing).
- 6.10 Locations for the deployment of LFR will be kept under strict review, with LFR being deployed into areas where it has the greatest potential to assist NWP in discharging its operational duties.
- 6.11 The decision to deploy LFR will always be supported by a rationale that explains why a location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other NWP LFR Documents.
- 6.12 Given that LFR requires a member of police personnel to review every Alert in real-time for a decision as to whether any further action is required, NWP will always deploy LFR in a way that is operationally effective and allows NWP to act on any Alerts as they are generated. **LFR will not be used indiscriminately.**

7. The LFR Deployment Process

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

- 1) LFR law enforcement purpose identified, safeguards considered, LFR deployment provisionally authorised by NWP NPCC Team.
 - 2) Consultation made with providing force, and authority given for Mutual Aid to be provided to NWP.
 - 3) Deployment authorised, and Watchlist selected;
 - 4) Notification of deployment, and signage deployed;
 - 5) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist;
 - 6) If a Possible Match is found in a Watchlist, the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the Watchlist are presented to the LFR Operator / LFR Engagement Officer for human review;
 - 7) The LFR Operator / LFR Engagement Officer will consider the Alert, noting the System, Subject and Environmental Factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is engaged;
 - 8) cancellation of authority for the LFR Deployment and post-deployment evaluation
- NWP Standard Operating Procedure provides a greater level of detail about the processes involved in the deployment of LFR by NWP.

7.2 Key Points

- a) LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are on a Watchlist;
- b) The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area;
- c) The quality and resolution of images (both those in the Watchlist and those from the video cameras) are of vital importance and must be carefully considered;
- d) The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.
- e) It is important to balance the objectives of the operation with the size of the Watchlist and the available resource to respond to Alerts. If the objectives are too broad and/or the Watchlist is too large, the amount of resource required to respond to Alerts may be prohibitively high.

7.3 Policing LFR Deployments Effectively

- 7.4 There must be sufficient appropriately trained resources deployed so as to be able to respond to Alerts. This is important in order to ensure that the LFR application, and the data processed by it, is being effectively used.

- 7.5 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, Recognition Time, and the probability of people from the Watchlist being observed by the camera (i.e occlusion) and their likely presence are all matters that must be considered when deciding what resources should be available.
- 7.6 It is also vital that NWP is transparent in its use of LFR under this guidance. As well as using signage, the provision of sufficient policing resources will allow officers to answer questions that the public may have.

8. Governance, Oversight and Impact Assessments

- 8.1 Following consultation the following stipulations have been proposed and accepted by NWP:-
- a) The overall benefits to the public must be balanced with public confidence of our use of LFR;
 - b) It can be evidenced that the technology itself will not result in unacceptable gender or racial accuracy variance into policing operations;
 - c) Each Deployment must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific policing purpose;
 - d) LFR Operators are trained to understand the risks associated with use of the LFR application, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions;
 - e) NWP, will develop and maintain robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency, whilst taking into account guidance from the Surveillance Camera and Biometric Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime
- 8.2 **Governance Framework**
- 8.3 NWP LFR Documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:-
- a) Pre-Deployment;
 - b) Operational Deployment;
 - c) Post-Deployment.
- 8.4 **Pre-Deployment**
- 8.5 Authority to deploy LFR is an operational one, where the NWP Authorising Officer (AO) rank is set at ACC or above. In exceptional cases of urgency, an officer below the rank of ACC, but not below the rank of Superintendent, may authorise the Deployment of LFR.

- 8.6 Where an officer below the rank of ACC provides the authority, an officer of the rank of ACC or above must be informed as soon as practicable. It is for the ACC or above to then authorise the deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.
- 8.7 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an NWP officer of NPCC rank (or police staff equivalent) must be engaged by the AO. Consultation at this level exists to expose the proposed deployment to an elevated level of strategic thinking, whereby issues are taken into account as much as possible. This affords NPCC the opportunity to scrutinise the deployment and to ask the AO to consider what mitigation is required to address concerns at hand.
- 8.8 The AO must notify the NWP Police and Crime Commissioner (or designated staff member) prior to any deployment.
- 8.9 The NWP Ethics Committee is an independent source of advice. Their terms of reference include the provision of advice and independent oversight of NWP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework. In continuing to monitor and develop our provision of this policing tactic, the Ethics Committee will be fully engaged and consulted.
- 8.10 Several specific NWP documents and records need to be completed in support of each deployment. These are set out as below:-

NWP LFR Deployment Specific Documents and Records	
LFR Application	Sets out the details of a proposed deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.
Written Authority Document	The AO's written authority provides a decision making audit trail demonstrating how the AO has considered the legality, necessity and proportionality of the deployment of LFR, the safeguards that apply and the alternatives that were considered but deemed to be less viable to realise the policing purpose. The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR deployment. The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.
LFR Deployment Record	Records details of where and when a deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.

Assessments	These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Surveillance Camera Commissioner's Self-Assessment. These documents need to be considered by the decision-maker when authoring a deployment to ensure they are sufficient to address the issues arising from the proposed deployment. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the deployment is not only necessary, but also proportionate to the policing purpose. Of note, the Surveillance Camera Commissioner's Self-Assessment will have been completed by the force providing the LFR technology, there is therefore no requirement for NWP to complete it. It should be available for AO review, if required.
Deployment Logs	Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.

- 8.11 Several other specific NWP documents pertaining to each NWP LFR deployment have been completed centrally. These are set out below:-

NWP LFR Documents and Records	
NWP Data Processing – Appropriate Policy Documents	NWP policy on the processing of data pursuant to the Data Protecting Act 2018 and UK General Data Protection Regulation relating to LFR.
NWP Legal Mandate	Outlines the legal considerations to be addressed in order to use LFR.

8.12 Operational deployment

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

- 8.14 The Silver Commander must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the deployment. The Silver Commander needs to be content:-

a) that the use of the LFR remains necessary and proportionate for the policing purposes identified in the Written Authority Document; and

b) that the safeguards identified in the written approval remain effective; and that the level of officer support committed to the deployment is enabling Alerts to be responded to effectively; and

c) that the Subject, System and Environmental Factors are such that the use of the LFR application remains effective for realising the policing purpose identified in the written approval.

8.15 Circumstances may arise that mean that there is a need to curtail or postpone the deployment. Examples may include occlusion resulting in those sought not being presented to the camera in cases of high crowd flow, adverse weather / lighting conditions or operational events changing the resources needed in the area. The Silver Commander must be empowered and have absolute discretion to suspend or terminate the deployment. Further details are provided within the LFR SOP.

8.16 In any event the Silver Commander must conduct and record a review of the activity at suitable intervals during the deployment. The timing and frequency of reviews is determined by the Silver Commander. A suitable period should be determined in the context of the deployment. This review should address the continued legality, necessity and proportionality of the deployment, as well as providing some analysis on LFR application performance and the engagements undertaken.

8.17 Post-Deployment

8.18 The use of LFR should be subject to debrief and review. This will help ensure that future deployments reflect learning identified from each deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the deployment.

8.19 Each deployment should be subject of an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO to ensure that appropriate senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

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

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

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

b) the data held on any 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 system generates an Alert all personal data is deleted as soon as practicable and in any case within 24 hours.

8.22 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

B) Investigations Act 1996; and /or

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

9. Oversight Bodies and Regulatory Framework

- 9.1 Within NWP, the senior internal oversight body for LFR is the NWP A.I ethics board, which in-turn will provide feed ins to the Trust, Confidence and Legitimacy Pillar, and to the Fit for the Future pillar, both of which are overseen by officers within the NPCC ranks. In addition, The NWP commissioner's office also provide an external oversight and scrutiny perspective.
- 9.2 The NWP LFR Legal Mandate sets out the legal framework for North Wales Police's use of LFR technology, whilst this LFR Policy Document and the NWP LFR Standard Operating Procedure supports implementation and effective use.
- 9.3 Nationally, the 'NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.
- 9.4 Further oversight opportunities may arise in relation to the 'Joint National Biometric Strategic Board'. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the Information Commissioners Office, the Surveillance Camera Commissioner, and the Biometric Commissioner. More detail on these roles:-

- a) Surveillance Camera Commissioner (SCC); The role of the Surveillance Camera Commissioner is to encourage compliance with the surveillance camera code of practice, review how the code is working, provide advice to ministers on whether or not the code required amendment.

Any usage of an LFR system by North Wales Police will need to comply with this Code and the twelve guiding principles. This guidance document seeks to apply those principles.

See www.gov.uk/government/organisations/surveillance-camera-commissioner

- b) Biometrics Commissioner (BC); The Commissioner is independent of Government and aims to keep the police use and retention of biometric data under review. The Commissioner makes decisions on applications made by the police to retain DNA profiles and fingerprints, and reviews national security determinations that are made or renewed by the Police in connection with the retention of DNA profiles and fingerprints. The Commissioner also reports to the Home Secretary about the carrying out of their functions.

See: www.gov.uk/government/organisations/biometrics-commissioner

- c) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Protection Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

10. Public Engagement

- 10.1 Public engagement should be supported by the use of online resources available to the public, which subject to the provisions around this contained within the Standard Operating Procedure, should be underpinned by a press and media strategy giving advance notice of deployments.
- 10.2 At and around the location of deployments, notices providing information, including details of the Privacy Notice, should be distributed and feedback via email should be sought.
- 10.3 Operational briefings delivered to officers and stakeholders prior to deployments should promote openness with the public and transparency about the use of LFR.
- 10.4 Officers should be encouraged to engage with the public to increase awareness of how LFR helps keep the public safe and how it helps bring offenders to justice. It is also helpful for officers to be in possession of information leaflets that can be handed out to the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.
- 10.5 The force Equality and Diversity lead should be consulted prior to any deployment.
- 10.6 NWP will seek to engage a community stakeholder group in advance of any deployments of LFR to gauge any community tension, concerns and worries and to allow NWP to take steps to address this and reassure our community if required.
- 10.7 Further details on public and community engagement can be found in the NWP LFR engagement strategy.
- 10.8 In Advance Of Deployments**
- 10.9 Prior to deployments, ensure that:
- a) Consideration is given to LFR Deployments being notified to the public using the NWP website and other appropriate communication channels (including social media). This should be standard practise, unless the AO decides that for operational reasons doing so in advance of the deployment would jeopardise the effectiveness of the policing purpose of the deployment.
 - b) LFR awareness raising measures (e.g. signs and/or leaflets) are prepared to support LFR Deployment in line with NWP LFR SOP; and
 - c) literature is prepared for persons who may be engaged (to include information outlined within a privacy notice); and
 - d) Officers are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a Constable in uniform to require a person to remove anything that conceals their identity; and

- e) external engagement is considered in discussion with the NWP LFR SPOC – currently an officer from within the NPCC Staff Office. It may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR SPOC must be consulted prior to this kind of activity.

10.10 During Deployments

10.11 During Deployments ensure that:-

- a) awareness raising measures are used in line with the NWP LFR SOP to ensure that 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; and
- b) notices with a brief explanation of LFR and reference to the NWP website are available to hand out to the public on request; and
- c) information is offered to persons engaged by officers in accordance with the standard operating procedure referred to above.

10.12 After Deployments

10.13 After deployments, ensure that:-

- a) information about the deployment, including location, time, date, number of Alerts, engagements, arrests, and any other information considered helpful and suitable for disclosure, is published on the NWP website. Care must be taken to ensure that no personal data is published;
- b) external engagement is considered in discussion with the NWP LFR SPOC. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR SPOC must be consulted prior to this kind of activity; and
- c) engagement with representatives from the Information Commissioners Office will be ongoing. This may be facilitated by NWP or by South Wales Police as the force supplying the LFR capability.

11. Watchlist Considerations
--

11.1 Image Quality

- 11.2** The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. The best images are those that follow a custody or passport style image that conforms to the NPIA 'Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'. Further detail is included within the following link: [Digital Images \(college.police.uk\)](https://college.police.uk/digital-images)

11.3 Where multiple images of a subject are available, consideration should be given to including these in the Watchlist where it is advised that they will improve the likelihood of locating those of interest to NWP.

11.4 **Compiling the Watchlist**

11.5 The NWP Legal Mandate provides commentary on the legal considerations relevant to compiling a Watchlist in a lawful way. This means that we ensure we hold the Watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes.

11.6 Key points include ensuring the Watchlist is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. The NWP LFR SOP provides practical guidance on this.

11.7 The size of the Watchlist is relevant to the level of resource that should be available to a deployment. There must be sufficient resources available to manage the Alerts generated by the LFR application.

11.8 As explained in section 5 (LFR Overview), Watchlists composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment. How great that likelihood needs to be will vary between cases for inclusion, but in any case should be considered against a number of factors. This means that an AO may deem it necessary and proportionate to authorise the inclusion of people to be included in a Watchlist, even though there may not be specific intelligence to say where in the North Wales Police force area they might be found. Factors for consideration in this respect include:-

- a) The severity of offence in question; this will often be relevant to the level of urgency associated with locating and arresting an individual. Many individuals change their behaviour, including the places they reside and frequent when they know that they are wanted for a serious offence;
- b) Risk; The level of risk associated with an individual or the offence type sought, whether that risk is to the public or themselves;
- c) Deployment location; the specific characteristics of the deployment location may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the Watchlist. Areas around transport hubs have a lot of people transiting from place to place.

11.9 **Governing the Watchlist**

11.10 The systems used to generate the Watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

11.11 NWP LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

11.12 Addressing Disproportionality

- 11.13 NWP does not create or retain a breakdown of race, gender or any other protected characteristic¹ of persons on a Watchlist. This mirrors the approach taken with the majority of policing tools used by NWP. The exception here is for inclusion of under 18's and under 13's as previously detailed.
- 11.14 The deployment of LFR is driven by North Wales Police's policing priorities and intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose that determines the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, there are realistic prospects of doing so, and that need fits with the policing purpose driving the LFR deployment.
- 11.15 The routine retention of data relating to protected characteristics would mean NWP holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a Watchlist.
- 11.16 NWP recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. Regular tests are carried out using police officers and staff volunteers who are 'seeded' into a 'Blue Watchlist'. The volunteers walk through the Zone of Recognition at the start of a Deployment to measure the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated.
- 11.17 As the provider of the LFR technology that NWP use, South Wales Police carries out academic equitability testing of the LFR system when necessary – such tests, including with the National Physical Laboratory have been documented. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.
- 11.18 When equitability tests are conducted, no biometric data belonging to members of the public is retained for the purpose of the tests. As part of these tests, a human operator monitors and records perceived gender, ethnicity, age and any other relevant protected characteristics, of persons passing through the Zone of Recognition during an LFR Deployment.
- 11.19 NWP has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts – i.e. being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:-
- a) those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and environmental Factors throughout the deployment. Should concerns arise that the LFR system is not performing correctly, the Silver commander will halt the deployment where necessary; and
 - b) for the purpose of facilitating post-deployment reviews, Alerts are retained for up to 24 hours. It provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in

¹ As defined in Section 4 of the Equality Act 2010

place for the Deployment, including the reviews undertaken by Silver and Gold during the Deployment; and

c) in the event post-deployment reviews identify an area of concern, NWP, or SWP as the force providing the LFR technology under the control of NWP, may undertake further equitability testing where this appears necessary.

12. Testing Equitability

- 12.1 In August 2021 South Wales Police was awarded Home Office Science, Technology, Analysis & Research (STAR) funding to undertake testing of the accuracy and equitability of FRT in an operational environment for LFR, OIFR and RFR.
- 12.2 In collaboration with the Metropolitan Police (MPS), this work was awarded to the National Physical Laboratory (NPL) at the end of 2021. The NPL is a prestigious world-leading centre of excellence that provides cutting-edge measurement science, engineering and technology to underpin prosperity and quality of life in the UK. In order to deliver on the objectives of the research, it was necessary to use and document the use of LFR in an operational setting within UK policing. Data collection for the evaluation took place in July and August of 2022 alongside five operational deployments of LFR, four in London and one in Cardiff.
- 12.3 A cohort of volunteers were selected to take part in the study who were of varying age, gender and race, the volunteers were seeded into the crowd passing the LFR System at each deployment so as to appear in the LFR video footage.
- 12.4 The data was then evaluated 'post event' with a balanced Watchlist and facial photographs taken of the volunteers in a variety of settings to realistically replicate the use cases for LFR, RFR and OIFR.
- 12.5 The full results are presented in the National Physical Laboratory's commissioned report 'Facial Recognition Technology in Law Enforcement Equitability Study'.
- 12.6 The NPL report gives us an impartial, scientifically underpinned, evidence-based robust analysis of the performance of the LFR FRT System used by NWP in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.
- 12.7 In summarising LFR operational performance, NPL have provided performance figures for two different Watchlist sizes: (i) a Watchlist of 10,000 reference images, which is broadly in line with those used on the MPS' LFR operational deployments to date and (ii) a watchlist of 1000 reference images a size more typical for SWP LFR deployments (examples of MPS and SWP figures are given, as these are the two forces in England and Wales who host LFR capability).
- 12.8 The performance figures use industry standard measures; (i) True-Positive Identification Rate (TPIR) (also known as True Recognition Rate)– the rate of successful recognition when subjects on the Watchlist pass through the Zone of Recognition (ii) False-Positive Identification Rate (FPIR) (also known as False Alert Rate) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the Watchlist pass through the Zone of Recognition

12.9 The table below shows the results of combined data from all five deployments:

Watchlist size 10000			Watchlist size 1000		
Metric	Threshold Setting	Result	Metric	Threshold Setting	Result
TPIR	0.60	= 89 %	TPIR	0.60	= 89 %
FPIR	0.60	≈ 0.017 % (1 in 6000)	FPIR	0.60	≈ 0.002 % (1 in 60,000)

12.10 In relation to LFR, NPL found that at a Threshold of 0.60, any differences in TPIR by gender, by race, or by race/gender combined were not statistically significant. **This means that the systems performance is not biased towards any race or gender.**

12.11 The study has shown that at Thresholds of 0.60, 0.62 and 0.64 the number of subjects with a false positive is very small and there is no statistically significant imbalance between demographics.

12.12 The study has shown that at a face match Threshold of 0.64 or higher there was no false positive identifications. Thus, at this Threshold the FPIR is identical for race, age and gender.

12.13 In relation to age, the NPL found that at a Threshold of 0.62 the observed differences in TPIR were not statistically significant. At a Threshold of 0.60, the observed variation in TPIR did show statistical significance with TPIR improving with subject age. This means that the system is slightly more likely to locate those sought as they age, but not more likely to inconvenience those of younger age, as the FPIR is found to be equitable between gender, race, and age. There is no statistically significant imbalance between demographics. In relation to trying to locate those of younger age, the NPL recognised;

“.....the lower performance of the under 20s is therefore assessed to be due to both demographic and environmental factors, these being a combination of subject age and as a result subject height, and crowdedness in the zone of recognition.....”

12.14 The result of this is that where NWP is particularly seeking to locate those of younger age and who may be of a shorter stature, consideration should be given to how busy the area is. The risk that subjects may be shielded from the camera by a taller person walking in front of them and blocking the camera's view must be taken in to account.

12.15 Therefore, deployment locations and camera positioning should form part of the technical optimisation process.

12.16 Reflective of the need for continuous improvement, NWP will continue to monitor our use of FRT performance, in terms of both overall system accuracy and demographic differential performance going forward.

13. Design Guidelines for LFR

13.1 A new international standard (ISO IEC 30137-1: 'Use of biometrics with video surveillance systems, Part 1: System design and specification') was published in May 2019. See www.iso.org/standard/64935.html

13.2 ISO IEC 30137-1 provides additional detail covering technical aspects of specifying and implementing a facial recognition system for use with video cameras, including camera selection and placement, adjustment of detection and matching Thresholds, Watchlist

management, and the role of the LFR Operator. It is strongly recommended that forces considering the use of LFR use the guidance to supplement the technical overview provided here. SWP has done this, and therefore by extension, NWP adheres to this by using SWP as providers for our LFR capability.

- 13.3 NWP LFR processes and associated guidance has been developed so as to provide for a reliable means of locating individuals using LFR with high definition CCTV cameras (2MP and above).
- 13.4 For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the LFR Operator, and associated policing resources on the ground.
- 13.5 A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this guidance.
- 13.6 Directly relevant components include:-
- a) the Cameras, including cabling, and their placement; and
 - b) the environment in which the cameras operate; and
 - c) the database of reference images and associated meta data, often referred to as the Watchlist; and
 - d) the facial recognition software that detects faces in the footage, converts the facial images into Templates, compares these against the Watchlist and provides information on the results of the comparison (generally in the form of an Alert or a numerical score) to an LFR Operator; and
 - e) the LFR Operator and LFR Engagement Officer who assess Alerts and determine the appropriate course of action; and
 - f) having sufficient officer resource to support the Deployment.
- 13.7 Ensuring that the design guidelines are adhered to, and that all directly relevant components are considered and in place will enhance the chances of the operation achieving its policing objective.

14. Cameras and Camera Placement

- 14.1 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.
- 14.2 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.
- 14.3 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.

- 14.4 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.
- 14.5 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).
- 14.6 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).
- 14.7 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.

15. Key Performance Metrics

- 15.1 This section covers some of the key performance metrics that should be gathered when deploying LFR. It outlines the minimum requirements and so additional metric or indicators may well be relevant and suitable for collation and analysis. There are two key metrics that determine the 'accuracy' of an LFR system. These are detailed in the below paragraphs.
- 15.2 **True Recognition Rate - TRR**
- 15.3 The number of times when individuals on a watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times when these individuals passed through the zone of recognition (regardless of whether an alert is generated).
- 15.4 This metric can only be generated by 'seeding' known subjects (for example police officers or staff) into a 'Blue Watchlist' and measuring the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated. Users of FR systems (and vendors) must not focus so closely on maximising this metric that they increase the False Alert Rate to inappropriate levels.
- 15.5 **False Alert Rate – FAR**
- 15.6 There are two types of False Alert Rate (FAR) measurements. The first is the System FAR, which is the number of False Alerts generated as a proportion of the total number of subjects processed by the LFR application. The second is the Operational FAR, which is calculated in the same way, but is measured after the LFR Operator has reviewed the output from the LFR application, and dismissed LFR application Alerts assessed by the LFR Operator as false.

- 15.7 All of the TRR and FAR metrics should be recorded and reported. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the FAR is greatly affected by the number of subjects processed by the LFR application, and to a lesser extent, the size of the Watchlist. This is a key reason why the number of persons included on the Watchlist needs to be kept as small as possible, whilst still meeting operational objectives.
- 15.8 It should be also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TRR and FAR. The Threshold needs to be set with care so as to maximise the probability of returning correct Possible Matches, whilst keeping the number of False Alerts to acceptable levels.
- 15.9 Recognition Time - RT**
- 15.10 A third important metric is the Recognition Time (RT). Note that the actual amount of time taken to act on an Alert will always be longer than the RT, as additional time is needed for the LFR Operator to assess the Alert and to pass to an LFR Engagement Officer to then make a final decision on whether to engage or not.
- 15.11 The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

16. LFR Guidance Summary

- 16.1 This guidance relates to the operational use of LFR, and the governance and oversight regimes necessary to support deployment.
- 16.2 It is strongly advised that officers and staff adhere to the guidance as this will help ensure that North Wales Police's use of LFR is both successful and lawfully serves the public, whilst providing necessary safeguards. Adherence is also key to maintaining the trust and confidence of the public, as well as the trust and confidence of our partners and other stakeholders.
- 16.3 It is recognised that circumstances may arise where for valid reasons, a decision is taken to do things slightly outside of this guidance. This will be for the individual making this decision to justify.

This guidance will evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are at odds with some aspects of this guidance, it is essential these decisions are fully documented, together with detailed rationale, and that the relevant decision-making is captured within the debrief and evaluation processes.

17. Acronyms used in LFR

AO	Authorising Officer
BC	Biometrics Commissioner

CCTV	Closed Circuit Television
CIA	Community Impact Assessment
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
EIA	Equality Impact Assessment
FAR	False Alert Rate
FR	Facial Recognition
FoIA	Freedom of Information Act
HRA	Human Rights Act 1998
ICO	Information Commissioner's Office
ISO	International Standards Organisation
LEA	Law Enforcement Agency
LFR	Live Facial Recognition
MOPI	Management of Police Information
SWP	South Wales Police
NPCC	National Police Chiefs' Council
NPL	National Physics Laboratory
NWP	North Wales Police
RT	Recognition Time
SCC	Surveillance Camera Commissioner
SCCSA	Surveillance Camera Commissioner's Self-Assessment
SOP	Standard Operating Procedure
TRR	True Recognition Rate
UK	United Kingdom
USB	Universal Serial Bus
VSS	Video Surveillance System
WAD	Written Authority Document
ZoR	Zone of Recognition



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

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:	

STANDARD OPERATING PROCEDURE

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	1
2.	Authority to deploy LFR	2
3.	'Where' - Considerations for date, time, duration and location of the deployment	4
4.	'How' - Measures during an LFR deployment.....	6
5.	'Who' - Watchlist generation and criteria for image inclusion on a Watchlist.....	7
6.	Management of risk and resource levels.....	16
7.	Planning and booking.....	17
8.	LFR operational roles	17
9.	Post Deployment	19
10.	LFR Application Security.....	20
11.	Data Retention & Data Management.....	21
12.	Contact Information.....	22
13.	Supporting documentation	22

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 necessary¹ 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

¹This 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....

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	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
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);	
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) 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 LFR², and these can be particularly relevant in relation to the above groups given their potential vulnerability³

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.

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.

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.		

Police originated images that may be included on a Watchlist

Images that may be deemed appropriate for inclusion within an LFR Watchlist include

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.

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 criteria. 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 be 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

	
Imagery	Layer A Layer B Layer C
Image Layer	Outline
Non-police originated image – Layer A	Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage; • circumstances where the police have obtained the image 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 ...

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 ...

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