SOUTH WALES POLICE
POLICY DOCUMENT FOR THE OVERT DEPLOYMENT OF
LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY

Protective marking:	Official
Publication scheme Y/N:	No
Title:	Policy document for the overt deployment of Live facial recognition (LFR) technology
Version:	Version 1.1
Summary:	Guidance for SWP Deployment of Live Facial Recognition Technology.
Department:	Digital Services Division
Review date:	03/03/2022

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	30.03.2021	Project Lead	Ch. Insp. Scott Lloyd	Initial Draft
0.2	14.06.2021	DSD SMT Review	Ch. Supt Simon Belcher	Minor Amendments
0.3	04.11.2011	Project Oversight	Ch. Insp Scott Lloyd	Minor Amendments
0.4	09.11.2021	DSD SMT Review	Ch. Supt Simon Belcher	No Amendments
1.0	11.11.2021	SRO Review	ACC Mark Travis	No Amendments
1.1	03.03.2022	Project Oversight	Ch. Insp Scott Lloyd	Minor Amendments

Table of Contents

Terms & Definitions: Capitalised terms used within this LFR Guidance Document shall have the meaning given to them in section 3 of this document unless otherwise defined.

1 Introduction, Aim and Scope

Introduction

1.1 Live Facial Recognition (LFR) technology helps South Wales Police 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 SWP uses it can be found in section 4 (LFR Overview).

1.2 This LFR Guidance Document provides SWP personnel with advice on the overt use of LFR in a legally complaint and ethical manner to enable SWP to achieve legitimate policing aims.

1.3 SWP is also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics Commissioner, and the Surveillance Camera Commissioner and has participated in the development of national guidance and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).

Aim & Scope

1.4 This guidance aims to: -

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

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

c) establish the governance structure for the Deployment of LFR, ensuring that SWP 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.

Not in Scope

1.5 There are other forms of facial recognition technology (FRT) that are <u>not</u> 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.

1.6 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 SWP 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 SWP's use of LFR – this is separately detailed within SWP's Legal Mandate document.

Additional Documents

1.7   A number of documents are available to supplement this guidance and these include but are not limited to, the:-

a) SWP LFR Standard Operating Procedure (SOP)

b) SWP LFR Data Protection Impact Assessment (DPIA)

c) SWP LFR Legal Mandate

d) SWP LFR Appropriate Policy Documents

e) SWP LFR Equality Impact Assessment

f) SWP LFR Training Documents and User Guides.

2   Terminology

2.1   Within SWP and throughout SWP 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).
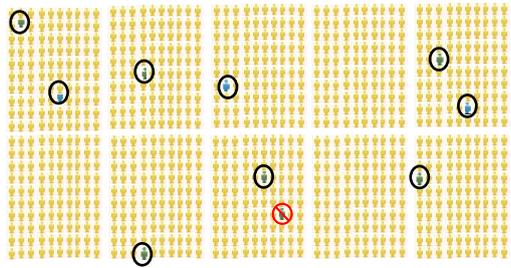
Confirmed False Alert
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

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 below. 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.
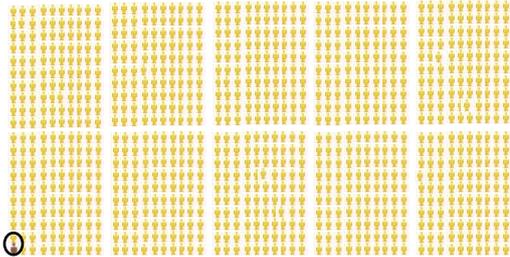
Authorising Officer (AO)

The officer officer (usually holds the rank of Superintendent 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

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 SWP deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of SWP 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.

3   LFR Overview

LFR in a Law Enforcement Context

3.1   Live Facial Recognition (LFR) technology helps South Wales Police locate people who are wanted for criminal offences and helps protect the most vulnerable in our society.

3.2   LFR also helps us locate those posing a risk of harm to themselves or others, 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.

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

LFR and SWP

3.4   LFR has been trialled by SWP over a period of four years. SWP believes that LFR is a valuable policing tool that helps SWP 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.

3.5   The following are illustrative examples where LFR may assist SWP 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.

3.6 Whilst appropriate use of LFR 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. SWP 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.

3.7 It is therefore incumbent on SWP 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.

3.8 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 and South Wales Police and Crime Commissioner's Office.

3.9 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. Each Deployment must be carefully designed and have clear documented objectives. The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality. Whilst considering proportionality, the AO should address how the public benefits from a Deployment and how this compensates for any concerns the public may have with regards to how their human rights are engaged.

3.10 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.

3.11 The AO must also consider how the Deployment 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.

3.12 SWP is not only concerned with developing and implementing policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. SWP will implement a robust governance process to review the effectiveness and impact of LFR Deployments on an ongoing basis. SWP 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 South Wales communities as part of an ongoing process.

3.13 This guidance document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

4. Strategic Intention, Objectives and Use Case

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

Strategic Intentions

4.2   SWP will:-

   a) use overt LFR technology in a responsible way to locate offenders in accordance with SWP's common law policing powers. This includes targeting those wanted for offences, and

   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 SWP'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 keep South Wales Safe.

   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 SWP LFR Documents; and

   g) transparently identify, manage and mitigate reputational and organisational risk to SWP; and

   h) be recognised as a progressive, responsible and ethical organisation.

Operational Objectives

4.3   SWP will:-

a) use LFR technology to enable SWP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities such as violent crime. LFR technology will increase intelligence-led enforcement opportunities including those relating to knife and gun crime, child sexual abuse, terrorism, and helping to safeguard vulnerable persons. It will also help locate those wanted by the courts or in breach of their bail conditions; 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.

Technological Objectives

4.4   SWP will:-

a) ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and

b) 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 SWP LFR SOPS under review. Where appropriate we will trial alternative providers of facial recognition software and hardware in parallel with our current provision. 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 previously detailed retention periods will remain unaffected.

Use of LFR

4.5   This guidance relates to the use of LFR in an overt capacity to help SWP protect the public. SWP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool.

4.6   LFR helps SWP use its resources more efficiently. SWP 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 SWP.

4.7   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 regards data protection should not be considered as an absolute barrier to information sharing).

4.8   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 SWP in discharging its operational duties. 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 SWP LFR Documents.

4.9   Given that LFR requires a member of SWP personnel to review every Alert in real-time for a decision as to whether any further action is required, SWP will always deploy LFR in a way that is operationally effective and allows SWP to act on any Alerts as they are generated. LFR will not be used indiscriminately.

5. Overview of LFR Deployment Processes

End-to-End Process

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

   a) LFR law enforcement purpose identified, safeguards considered, Deployment authorised, and Watchlist selected;
   b) Notification of Deployment, and signage deployed;
   c) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist;
   d) 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;
   e) 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;
   f) Cancellation of authority for the LFR Deployment and post-Deployment evaluation.

5. 2   SWP LFR SOP provides a greater level of detail about the processes involved in the Deployment of LFR by SWP. A flowchart summarising LFR Deployment can be found in Section 13 of this document.

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. The numbers on a Watchlist will therefore need to be as small as possible, whilst still achieving the legitimate policing purpose. The size of the Watchlist will typically not exceed a thousand;

   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.

Policing LFR Deployments Effectively

5.3   There must be sufficient appropriately trained resource 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.

5.4   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 are all matters that must be taken into account when deciding what resources should be available.

5.5   It is also vital that SWP is transparent in its use of LFR under this guidance. As well as using signage, the provision of sufficient policing resource will allow officers to answer questions that the public may have.

6. Governance, Oversight and Impact Assessments

6.1   Following consultation the following stipulations have been proposed and accepted by SWP:-

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)   SWP, 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.

Governance Framework

6.2   SWP 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.

Pre-Deployment

6.3   Authority to Deploy LFR is an operational one, where SWP Authorising Officer (AO) rank is set at Superintendent. In exceptional cases of urgency, an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR.

6.4   Where an officer below the rank of Superintendent provides the authority, a Superintendent must be informed as soon as practicable. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.

6.5   Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents <u>must</u> be completed and an SWP officer of NPCC rank[1] (or police staff equivalent) <u>must</u> be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby 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.

6.6   The AO must notify the SWP Police and Crime Commissioner (or designated staff member) prior to any deployment.

6.7   SWP Ethics Committee are an independent source of advice. Their terms of reference include the provision of advice and independent oversight of SWP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework.

---

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

6.8 A number of specific SWP documents and records need to be completed in support of each Deployment. These are set out below:-

SWP 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, the safeguards that apply to the Deployment 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.
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.

6.8 Several other specific SWP documents pertaining to each SWP LFR Deployment have been completed centrally. These are set out below:-

SWP LFR Documents and Records	
SWP Data Processing – Appropriate Policy Documents	SWP policy on the processing of data pursuant to the Data Protecting Act 2018 and UK General Data Protection Regulation relating to LFR.
SWP Legal Mandate	Outlines the legal considerations to be addressed in order to use LFR.
SWP Training Materials	Provides the necessary training to ensure those involved in authorising and deploying LFR are familiar and implement the considerations relevant to its lawful, ethical and appropriate use.

Operational Deployment

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

6.10 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

   c) that the level of officer support committed to the Deployment is enabling Alerts to be responded to effectively; and

   d) 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.

6.11 Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples may include insufficient footfall or poor light conditions. The Silver Commander must be empowered and have absolute discretion to suspend or terminate the Deployment. Further details are provided within the LFR SOP.

6.12 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.

Post-Deployment

6.13 Once a Deployment is concluded, it should of 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.

6.14 Each Deployment should be subject of an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO (this may be the same person as the Silver Commander) to ensure that appropriately senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.

6.15 The outcome of LFR Deployments must be subject of evaluation, which in turn should feed into oversight and scrutiny processes.

6.16 Post-Deployment, SWP must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with SWP 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.

6.17 Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 24 hours.

6.18 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 SWP's complaints / conduct investigation policies.

7. Oversight Bodies and Regulatory Framework

7.1 Within SWP, the senior internal oversight body for LFR is SWP FRT & Biometrics Programme board, which in-turn answers to DSD Gold Board. In addition, The SWP commissioner's office also provide an external oversight and scrutiny perspective.

7.2 SWP LFR Legal Mandate sets out the legal framework for SWP use of LFR technology, whilst SWP LFR Policy Document and SWP LFR SOP support implementation.

7.3 Nationally, the `NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.

7.4 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 SWP LFR system 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.

   See www.gov.uk/government/organisations/information-commissioners-office.

8. Public Engagement

8.1 Public engagement must be supported by the use of online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of Deployments. 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.

8.2 Operational briefings delivered to officers and stakeholders prior to Deployments should promote openness with the public and transparency about the use of LFR. 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 notices that can be handed out to the public. Such notices should deliver important key messages aimed at promoting trust and confidence through improved understanding.

8.3 Key stakeholders, including the PCC's Office, may be invited to observe the planning and Deployment of LFR.

In Advance of Deployments

8.4 In advance of Deployments ensure that:-

a) LFR Deployments are notified to the public using SWP website and other appropriate communication channels (including social media); and

b) LFR notices and leaflets are prepared to support LFR Deployment; 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 compel a person to remove anything that conceals their identity; and

e) external engagement is considered in discussion with SWP LFR team. 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 team must be consulted prior to this kind of activity.

During Deployments

8.5 During Deployments ensure that:-

a) signs are clearly and prominently displayed beyond the curtilage of the Zone of Recognition for the LFR cameras to state that a Deployment is underway and to give details of how the public may access further information; and

b) notices with a brief explanation and reference to SWP website are available to hand out to the public on request; and

c) information is provided to persons Engaged by officers in accordance with the policy referred to above.

After Deployments

8.6 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 SWP website. Care must be taken to ensure that no personal data is published;

b) external engagement is considered in discussion with SWP LFR team. 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 team must be consulted prior to this kind of activity; and

c) engagement with representatives from the Information Commissioners Office will be ongoing.

9. Watchlist Considerations

Image Quality

9.1   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 embedded PDF:

NPIA Standard Still
Digital Images.pdf

9.2   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 SWP.

Compiling the Watchlist

9.3   SWP 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.

9.4   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. SWP LFR SOP provides practical guidance on how to follow SWP LFR Documents, including SWP Legal Mandate.

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

9.6 As explained in section 3 (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 wanted by SWP for serious offences such as murder, rape, kidnap, GBH (etc.) to be included in a Watchlist, even though there may not be specific intelligence to say where in SWP they might be found. Some of the factors for consideration include:-

a) 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, 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. Areas around transport hubs have a lot of people transiting from place to place.

Governing the Watchlist

9.7 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.

9.8 SWP 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.

Addressing Disproportionality

9.9 SWP does not create or retain a breakdown of race, gender or any other protected characteristic[2] of persons on a Watchlist. This mirrors the approach taken with the majority of policing tools used by SWP. The exception here is for inclusion of under 18's and under 13's as previously detailed.

9.10 The Deployment of LFR is driven by SWP policing priorities, 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, and that need fits with the policing purpose driving the LFR Deployment.

9.11 The routine retention of data relating to protected characteristics would mean SWP 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.

---

[2] As defined in Section 4 of the Equality Act 2010.

9.12 SWP 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.

9.13 SWP also carries out academic equitability testing of the LFR system when necessary. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

9.14 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.

9.15 SWP has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. For example, 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 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, SWP may undertake further equitability testing where this appears necessary.

10. Design Guidelines for LFR

10.1   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.

10.2   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.

10.3   SWP 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). 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.

10.4   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. 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.

11. Cameras and Camera Placement

11.1 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.

11.2 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.

11.3 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. This also needs to take into consideration the requirement to view across a large moving crowd.

11.4 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.

11.5 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).

11.6 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).

11.8 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.

12. Key Performance Metrics

12.1 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.

True Recognition Rate

12.2 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).

12.3 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.

False Alert Rate FAR

12.4 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.

12.5 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.

12.6 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.

Recognition Time

12.7 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.

12.8 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.

13. LFR Guidance Summary

13.1 This guidance relates to the operational use of LFR, and the governance and oversight regimes necessary to support Deployment.

13.2 It is strongly advised that officers and staff adhere to the guidance as this will help ensure that SWP use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.

13.3 It is recognised circumstances may arise where for valid reasons, a decision is taken that it is necessary to things slightly outside of this guidance. This guidance will no doubt 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 features within debrief and evaluation processes.

14. 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
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