GREATER MANCHESTER POLICE

Deployment of Overt Live Facial Recognition Technology

Policy

10th Oct 2025

DATE THIS VERSION IMPLEMENTED: October 2025

DATE NEXT REVIEW IS DUE: October 2026

CHIEF OFFICER SPONSOR: ACC Jackson (Crime, Forensics & Intelligence)

POLICY OWNER: DCS Jones (Interim Head of Intelligence Branch)

POLICY AUTHOR: Insp Middleton (FIB) / Ch.Insp Booth (Change Branch)

APPROVED BY: ACC Jackson (via Project Board)

GOVERNMENT SECURITY CLASSIFICATION: Official

IS THE POLICY NEW OR REVISED: New

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)	PUBLISHED ON CCOs
1.0	1/11/24	New policy	Insp Jon Middleton	N/A
1.1	6/4/25	New policy draft updated follow consultation with minor amendments throughout as per comments section	Insp Jon Middleton	N/A
1.2	11/7/25	Draft updated following further reviews and comments	Insp Jon Middleton	N/A
1.3	15/09/25	Minor amendments throughout and new sections re use-case within overall aims	Ch.Insp Booth	N/A
1.4	10/10/25	Updates to GSB comments, requirements for DEI data capture pending updates to IT Watchlist tool	Ch.Insp Booth	N/A
1.5	16/10/25	Inclusion of consultation feedback re policy	Ch.Insp Booth	

Table of Contents

1. Policy Statement

Deployment of Live Facial Recognition (LFR) will largely fall into one of three use cases outlined below. It will be for the applicant and the Authorising Officer (AO) to assess the necessity and proportionality of the LFR Deployment in line with Authorised Professional Practice (APP) (College of Policing website) however, each LFR Deployment will need:

- A review of the intelligence case surrounding each request for the Deployment.
- A review to ensure that all images meet the necessity and proportionality criteria for inclusion.
- Consideration that the watchlist is not excessive for the purpose of the LFR deployment itself.
- That the watchlist 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.
    - 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 – the source of the image should be recorded.
- The watchlist should 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.
    - 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 should be paid to the prospect of the LFR system generating an alert if an older image is proposed for inclusion, where the person's facial features may have changed or aged significantly since the image was taken.
- The watchlist should be imported into the LFR system immediately prior to deployment and no more than 24 hours prior to the commencement of the deployment, to ensure that the watchlist is current – where the deployment is to last in excess of 24 hours, force procedures should require an ongoing review of the watchlist, covering the issues of review, retention and deletion.

Images that may be deemed appropriate for inclusion within an LFR watchlist include custody images of individuals and/or other police-originated images of people who are:

- wanted by the courts
- 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
- subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the deployment
- missing persons deemed at increased risk of harm (as defined by APP – for GMP all medium and high risk missing persons)
- presenting a risk of harm to themselves or others
- a victim of an offence or a person who the police have reasonable grounds to suspect would have information of importance and relevance to progress an investigation, or who is otherwise a close associate of an individual and that individual would fall within people wanted by the courts and presenting a risk of harm to themselves or others

This will lead to three overarching types of deployments:

a) Proactive Deployments: These are routine deployments of LFR to locations within GMP. These Deployments will be based on information and intelligence and crime data for those areas, including increases in types of crime and persistence of crime occurring at significant volumes at a given location. These deployments will be focused around locations and access routes where LFR will provide the most benefit in discharging the operational duties of GMP. Watchlists will be linked to the purposes of the Deployment and there should be a reasonable suspicion that Subjects included in Watchlists may attend at the Deployment location.

b) Event Deployments: These Deployments are in response to specific events which are expected to attract increased public attendance to an identified location. These Deployments will support policing operations to ensure the safety of the public at the location. This will also include transport hubs and routes that can be identified as supporting attendance to the specified event. Watchlists will be compiled based upon the location and nature of the event.

c) Incident/ Intelligence specific Deployments: These Deployments will be in response to a specific incident or in response to specific intelligence. The Watchlists for these Deployments will be limited to the geographical location of the Deployment and include individuals based on the specific needs of the incident response or intelligence. An example of this would be Deployment of LFR to a location where disorder has recently occurred and intelligence exists that the disorder may continue between identified individuals who have yet to be located. Another example would be where we could reasonably expect that a missing person (medium / high risk) may be located withing a Deployment area.

This document explains the policy and procedures to be adopted when planning for deployment of, using operationally & reviewing Live Facial Recognition (LFR) technology in support of policing operations.

1.1 Aims

i. To provide an overview of LFR technology and its use for GMP officers, staff & the public.
ii. To establish a governance structure for deployment of LFR in GMP, ensuring that GMP's use of LFR is legally compliant and accountable.
iii. To provide policy guidance on planning LFR deployments.
iv. To provide policy guidance on using LFR operationally.
v. To provide policy guidance on reviewing use of LFR.

2. Scope

i. All operational officers and staff, and their supervisors involved in the planning and deployment of LFR.
ii. All officers and staff involved in any subsequent investigation resulting from the operational deployment of LFR technology.
iii. All authorising officers (AOs)

iv. All officers applying for the deployment of LFR.
v. The operational command team for LFR deployment (Gold, Silver and Bronze)
vi. LFR operators, LFR engagement officers and LFR system engineers.

This document does not cover the use of:

i. Retrospective Facial Recognition (RFR) – retrospective searching of video/still images.
ii. Operator Initiated Facial Recognition (OIFR) – human initiated facial search from a mobile device.
iii. Covert use of LFR

3. Terms and Definitions

Adjudication - a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed, by the LFR Operator) to decide whether to Engage 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. The Administrator may also be referred to as the LFR System Engineer.

Alert - an alert is generated by the LFR system when a facial image from the video stream, which is being compared against the Watchlist, returns a comparison with a similarity score above the set Threshold.

True Alert - When it is determined that the Probe Image is the same as the Candidate Image in the Watchlist.

Confirmed True Alert - following an Engagement, it has been determined that the Engaged individual is the same as the person in the Candidate Image in the Watchlist.

True Recognition Rate – (also known as the True Positive Identification Rate) – This describes the total number of times an individual(s) known to have passed through the Zone of Recognition and correctly generated an Alert, as a proportion of the total number of times the same individuals pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR system or not. By way of an example, the 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. The same would be true if 5 people each pass the LFR system twice, and 2 Alerts were correctly generated for 4 of the people and only 1 correct Alert for the 5th person.

False Alert - it is determined that the Probe Image is not the same as the Candidate Image in the Watchlist, based on Adjudication without any Engagement.

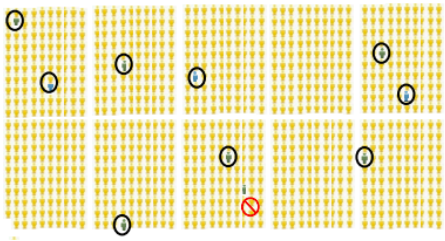
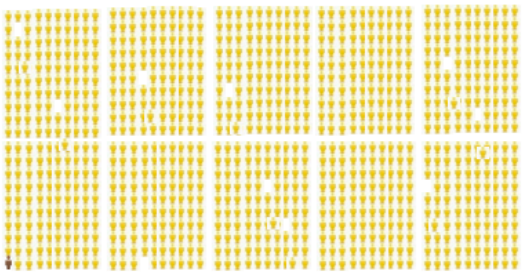
Confirmed False Alert - following an Engagement, it has been determined that the Engaged individual is not the same as the person in the Candidate Image in the Watchlist.

False Alert Rate – (also known as the False Positive Identification Rate). This describes 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.

Application – the GMP LFR application/authorisation form.

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.

	True Recognition Rate	False Alert Rate
What is it?	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.	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 who provides the authorisation for LFR to be Deployed. LFR may not be used without this authorisation.

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. Note that Templates are proprietary to each facial recognition algorithm and new Templates will need to be generated from the original images if the algorithm is changed.

Blue Watchlist - a watchlist comprising of 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 at the start of a Deployment to measure the True Recognition Rate.

Cancellation Report - the GMP LFR application/authorisation form part 3.

Candidate Image - the image of a person from the Watchlist returned as a result of an Alert.

Crime Hotspot - a small geographical area where crime data and/or intelligence reporting and/or operational experience as to the current and future criminality indicates that that it is an area where crime/incidents/events are disproportionately concentrated and/or the crime rate and/or the rate at which crime in that area is rising.

Deployment - use of an LFR system as authorised by an AO to locate those on an LFR Watchlist.

Deployment record - 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 - occurs when an officer communicates with a member of the public as a result of an LFR Alert. The term 'Engagement Officer' shall be construed accordingly.

Environmental Factor - an external element that affects LFR system performance such as dim lighting, glare, rain, mist etc.

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.

Live Facial Recognition (LFR) - 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 with suitable technical qualifications and experience to optimise and maintain the operational capability of the GMP LFR system.

Missing Persons Hotspot - A small geographical area where intelligence reporting and/or operational experience indicates missing persons are likely to be present.

GMP LFR Documents - the GMP LFR Policy & Procedure, Legal Mandate, and the associated impact assessments.

Overt Live Facial Recognition – use of Live Facial Recognition in a manner that can readily be detected by those members of the public who may be affected by it, particularly through the use of awareness raising measures detailed elsewhere in this document. This document is not concerned with any possible use of LFR authorised by way of the Regulation of Investigatory Powers Act 2000.

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 - the facial image submitted for a facial search against the Watchlist.

Protective Security Operation - a specific security operation aimed at keeping the public safe and/or protecting property or national infrastructure.

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.

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.

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

Sought Persons - persons included on an LFR Watchlist.

Subject Factor - a factor linked to the individual. 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 system 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 correct suggested matches whilst keeping the number of False Alerts to an acceptable level.

(NB. It should be noted that any FR algorithm is only returning 'suggested' matches, based on the chosen Threshold, and that it is for a human to assess the true likelihood that the images relate to the same person).

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 opportunities with limited time to act, where the seriousness and potential benefits support the urgency of action.

Use Case – The reason GMP need to locate Sought Persons.

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.

Written Authority - the GMP LFR application/authorisation form.

Zone of Recognition (ZoR) - the 3-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, for example 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.

4. LFR overview

i. LFR technology uses a live camera feed to scan facial images of a crowd and uses advanced algorithms to instantly check against a pre-determined watchlist. If the facial image is not on the watchlist then the image is disregarded / deleted immediately.

ii. LFR has been trialled by South Wales Police and the Metropolitan Police for a number of years. In seeking to address concerns regarding use of the technology, South Wales Police facilitated academic research led by the National Physical Laboratory and has proactively engaged with civil liberty interest groups and SWP Police and Crime Commissioner's Office. The research has offered reassurance regarding the use of LFR and whether it will perform differently in relation to different demographics. GMP have the results of this research and a copy can be found in section 16 of this document and is also available on GMP's website facial recognition page.

iii. 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 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 GMP personnel who then decides as to whether any further action is required. In this way, the LFR application works to assist GMP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

iv. 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 and 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 because of LFR processing.

v. GMP will 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 using LFR.

5. Strategic Intention

i. Use LFR technology in a responsible way to locate people in accordance with GMP common law policing powers. This includes targeting those wanted by the courts and those wanted for criminal offences. GMP will focus on its policing priorities aligned to the Plan on a Page and the Force Control Strategy. These include tackling violent and other serious crimes, with a particular regard to knife and gun crime, child sexual exploitation and terrorism.

ii. Strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep Greater Manchester safe for everyone.

iii. Build public trust and confidence in the development, management, and use of LFR by taking account of privacy concerns and maximising transparency.

iv. Maintain good governance through a command structure that incorporates strategic, tactical, operational, and technical leads for the deployment of LFR, with clear decision making and accountability.

v. Ensure that the deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework.

vi. Transparently identify, manage, and mitigate reputational and organisational risk to GMP.

vii. Be recognised as a responsible, exemplary, and ethical organisation.

6. Tactical and Operational Objectives

i. Use LFR technology to enable GMP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities such as violent and other serious 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.

ii. 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 to act.

iii. Engage with and provide reassurance to communities, listening and responding to concerns.

iv. Both locally and through National Frameworks identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

7. Technological Objectives

i. Ensure all LFR technology we use is fit-for-purpose and deployed effectively in line with strategic intentions and tactical/operational objectives.

ii. Provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic.

iii. Scan the horizon to explore potential improvements in the technology.

8. Use of LFR

i. GMP's LFR system is a dedicated CCTV system delivered via CCTV equipment on a liveried vehicle/s deployed in a static location.

ii. LFR allows GMP to use its resources more efficiently. LFR is better than humans at recognising persons from a large dataset and quickly linking a possible match, whilst providing information that indicated why they may be of interest to GMP.

iii. In some circumstances use of LFR can help minimise information sharing, as LFR offers an alternative to media appeals, or the sharing of information with external agencies. (It is acknowledged that data protection should not be considered as an absolute barrier to information sharing).

iv. 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 GMP in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why a location was selected in accordance with the principles set out in the Legal Mandate and other GMP LFR Documents.

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

vi. The process for deployment of LFR in GMP is detailed in the GMP Live Facial Recognition Procedure.

9. Overview of LFR deployment procedure

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

i. LFR law enforcement purpose identified, safeguards considered, deployment authorised, and Watchlist selected.

ii. Notification of deployment, and signage deployed.

iii. Deployment - as subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist.

iv. 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.

v. 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.

vi. Cancellation of authority for the LFR deployment and post-deployment evaluation.

The GMP LFR Procedure document provides a greater level of detail about the processes involved in the deployment of LFR by GMP.

10. Governance and oversight

Governance and operational oversight of the use of the technology is approached in three stages:

Stage 1: Pre-Deployment
Stage 2: Operational Deployment
Stage 3: Post-Deployment

10.1 Stage 1: Pre-Deployment

a) An officer must seek the authorisation to deploy LFR using the GMP LFR application form.

b) The grounds to deploy LFR may give rise to the need for a single Deployment, or a need for a series of deployments which share a common ‘thematic’ purpose save that any series of deployments may not endure beyond a 7-day period. Should the need for deployment continue beyond 7 days, a further GMP LFR application form authority must be granted. This approach ensures that the use of LFR is time limited but allows an operationally effective way to plan for and deliver LFR in conjunction with other operational tactics across Greater Manchester.

c) The authority to deploy LFR is provided by a GMP authorising officer (AO), an AO is to be of at least the rank of Superintendent and have completed recognised LFR AO training.

d) Where an AO is not immediately able to provide their decision in writing and the authorisation needs to granted urgently, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable using the GMP LFR application form.

e) Situations where the need for an authorisation to be granted urgently would include:

(i) an imminent threat-to-life or an imminent threat of serious harm to people or property; and / or
(ii) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which supports the urgency of action.

f) Prior to AO authorisation, the below documents must be completed and provided to the AO for review:

(i) GMP LFR application form.
(ii) A review of the Force Level Community Impact Assessment and Equality Impact Assessment should be completed and documented. Where necessary a bespoke local CIA should be created and submitted as part of the application. This will be for the Authorising Officer to consider the necessity for a local CIA.

g) Prior to any Deployment the following must be informed of the deployment by the LFR team on behalf of the AO (or the AO themselves in urgent cases):

- Force Duty Assistant Chief Constable via Force Operations Centre (directly in urgent cases)
- Office of Deputy Mayor for Safer & Stronger Communities
- The deployment applicant.
- An officer of the rank of Superintendent or above for the District where the deployment is taking place (if not already the AO or applicant) or if none available the Duty Superintendent for that geographical area.
- Criminal Justice & Custody Branch

10.2 Stage 2: Operational Deployment

a) During the operational deployment, a log must be completed to record the planning and execution of the Deployment. Where any event GSB is in place the operational LFR team will work to the Gold and Silver strategy documented. For routine deployments the District Superintendent will assume the role of Silver Commander with the Duty ACC assuming the role of Gold Commander.

b) A Silver Commander shall, in conjunction with Bronze, review the use of LFR for the duration of the Deployment to ensure that they remain satisfied that the use of LFR remains necessary and proportionate for the policing purpose identified, all identified safeguards remain effective, and Alerts are being responded to effectively, Subject, System and Environmental Factors are such that the use of the LFR system remains effective.

c) The Silver Commander must be empowered and have absolute discretion to suspend or terminate the Deployment.

d) The Bronze Commander, for each deployment, will be a member of the LFT operational team who must conduct and record a review of the activity at suitable intervals during the Deployment at a time and frequency determined by the Gold Commander. The review by the Bronze Commander should address the continued legality, necessity, and proportionality of the Deployment, as well as providing some analysis on LFR system performance and the Engagements undertaken. The Bronze Commander must report the output of their review to Silver.

10.3 Stage 3: Post-Deployment

a) Following each LFR Deployment debrief, a review shall be conducted, to ensure future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.

b) The retention of the CCTV for up to 31 days provides a means by which Alerts can be retrospectively reviewed by technical analysts to inform the future configuration of the LFR System.

c) Post-deployment the following forms shall be completed:

(i) GMP LFR application form Part 3 – Cancellation report. The LFR Cancellation Report is submitted to the AO within 31 days of the date of the Deployment. These will be periodically reviewed by the SRO and the GMP FR Board to consider effectiveness and trend, as well as oversight and scrutiny.
(ii) An entry on the register of Deployments.

10.4 Register of Deployments

Any Deployment of LFR must be recorded on a centrally held register. This register will record:

a) name and rank of the AO and command team.
b) date, time, duration, and locality of Deployment.
c) watchlist details around overall number (further IT development work required to capture further DEI characteristics – however full details will be kept of those subjects engaged with as part of an operational deployment.)
d) number of Alerts, broken down as True Alerts and False Alerts, including:
    (i) perceived age range
    (ii) perceived sex
    (iii) perceived race (by reference to Policing IC Code)
e) number of Engagements and their results

10.5 Oversight arrangements

i. Internal oversight for LFR is provided by GMP's FR working group, chaired by the FR SRO, which meets monthly. This working group answers in turn to the Serious Crime Board chaired by ACC Crime, Intelligence and Forensics.

ii. Part of GMP's FR working group terms of reference is the reviewing of LFR Deployments on a monthly frequency to monitor for trends and direct changes for best practice. Aggregated demographic data will also be considered at these

meetings and take steps as required to ensure GMP continues to discharge is Public Sector Equality responsibilities.

iii. Further oversight is provided by the GM Deputy Mayor for Safer & Stronger Communities and Greater Manchester Independent Ethics Committee who are briefed on LFR deployments by GMP's FR SRO on a quarterly basis.

iv. Additional oversight is provided by other regulatory bodies, including the Biometrics and Surveillance Camera Commissioner, the Information Commissioner's Office, and the Equality and Human Rights Commissioner.

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

vi. 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.

11. Data management

11.1 Data retention

GMP will ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the other LFR documentation. This means that:

a) where the LFR system does not generate an Alert, that a person's biometric data is immediately automatically deleted by the LFR software.

b) The LFR Watchlist will be deleted as soon as reasonably practicable, and in any case within 24 hours, following the conclusion of the Deployment.

c) Where the LFR system generates an Alert, all related personal data is deleted as soon as practicable and in any case within 24 hours , except to the extent that:

(i) personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996.
(ii) personal data is retained in accordance with GMP's complaints / conduct investigation policies.

d) The CCTV footage generated from LFR Deployments will be deleted within 31 days, except to the extent that the footage is retained:

i. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996.
ii. in accordance with GMP's complaints / conduct investigation policies
iii. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure

data subjects are informed as to the arrangements that will apply to the use and retention of such data.

e) To support compliance the LFR system has a full audit capability, and the LFR log is retained in accordance with MOPI.

f) 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 GMP's Data Protection Officer.

11.2 Data security

The LFR system includes several physical and technical security measures including:

- Images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine.
- The LFR system is a closed-circuit TV system that implements defences in depth principles to protect the application and related data.
- The LFR system is physically protected when in use and securely wiped following each Deployment.
- A full audit is maintained of all user initiated actions undertaken during the course of a Deployment.
- Technical issues with the LFR system will be dealt with by LFR System Engineers deployed on the operation.

12. Transparency & reporting

i. Public engagement should be underpinned by a communications 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.

ii. Operational briefings delivered to officers and stakeholders prior to Deployments should promote openness with the public and transparency about the use of LFR.

iii. 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.

iv. Key stakeholders should be invited to observe the planning and Deployment of LFR where possible.

12.1 Policy & documentation

This policy & procedure, associated impact assessments and wider information (including a frequently asked questions section) are available on GMP's website.

12.2 Stage 1: Pre-Deployment

The public will be notified of LFR deployments in advance using GMP's website and other appropriate communication channels (for example – social media). In exceptional circumstances it may not be possible to give prior notice of the use of LFR, for example in cases of Urgency and/or in relation to use concerning specific intelligence where the source of that intelligence or the operational objectives for the use of LFR risk being compromised.

12.3 Stage 2: During deployment

Measures will be taken during the deployment to ensure the use of LFR is overt such that members of the public in the vicinity of the particular LFR deployment are in a position to recognise and understand that LFR is being used and to seek information about the operation of LFR from officers. Such measures will include:

(i) Trained engagement officers to provide information to the public.
(ii) Liveried Police vehicle(s)/hoardings with signage on them informing on the use of LFR
(iii) Signage or an equivalent measure (e.g. some locations may use alternatives such as PA announcements) outside the Zone of Recognition.

Any member of the public who is engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. This may not be possible should the person have left before the leaflet could be offered or its provision would engage a restriction under Section 44(4) – (6) of the Data Protection Act 2018.

Any person who requires further information relating to LFR should be provided with contact information for the GMP Facial Recognition team facial.recognition@gmp.police.uk

12.4 Stage 3: Post-Deployment

A record of deployments will be published on the GMP website. This will confirm for each Deployment:

i. Deployment location
ii. Date of the Deployment
iii. Duration of the Deployment
iv. Whether the Deployment was to a crime hotspot, missing person hotspot, to support a PSO and/or following specific intelligence.
v. Watchlist size
vi. The minimum threshold setting.
vii. Total Alerts
viii. The number of Confirmed True Alerts and Confirmed False Alerts,
ix. The number of unconfirmed True Alerts and False Alerts,
x. The False Alert Rate
xi. Estimated faces passing the LFR system.

12.5 Wider information

On an annual basis, a report will be provided on GMP use of LFR including how it has been used, details as to Watchlist composition and the results gained. The report will also provide

demographic analysis relating to the Watchlist composition and the Alerts, the results gained.

Additionally, requests can be made under the Freedom of Information Act 2000, or in relation to the exercise of individual rights pursuant to the Data Protection Act 2018.

13. Watchlist considerations

13.1 Image Quality

i. 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)'. This document can be found in section 16.

ii. 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 GMP.

13.2 Compiling the Watchlist

i. The GMP 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.

ii. 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 GMP LFR Procedure document provides practical guidance on how to follow GMP LFR Documents, including the Legal Mandate.

iii. 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.

iv. Watchlist composition will be proposed by the applicant and considered by the Authorising Officer in terms of the proportionality, necessity, legality and intrusion of inclusion. Where practicable, a watchlist should focus on subjects that are likely to be located within the deployment area.

v. Factors for consideration in this respect 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 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.

13.3 Governing the Watchlist

i. 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.

ii. GMP 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.

13.4 Addressing Disproportionality

i. GMP will not create or retain a breakdown of race, gender, or any other protected characteristic (as defined in section 4 of the Equality Act 2010) of persons on a Watchlist, (not technically possible at this time), but will retain records for those engaged with on deployment.

ii. The Deployment of LFR is driven by GMP 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, there are realistic prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.

iii. The routine retention of data relating to protected characteristics would mean GMP 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.

iv. GMP 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.

v. GMP will carry out academic equitability testing of the LFR system when necessary – such tests, including with the National Physical Laboratory, have been documented previously by other Police forces. The necessity and frequency are determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

vi. 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.

vii. GMP 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:

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, GMP may undertake further equitability testing where this appears necessary and will notify relevant key stakeholders.

14. Camera configuration & placement

i. 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.

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

iii. 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.

iv. 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.

v. 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).

vi. 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).

vii. 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

This section covers some of the key performance metrics that GMP will record when deploying LFR. It outlines the minimum requirements and additional metrics, 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.

15.1 True Recognition Rate

i. 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).

ii. 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.

15.2 False Alert Rate (FAR)

i. 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.

ii. 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.

iii. It should 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 to maximise the probability of

returning correct Possible Matches, whilst keeping the number of False Alerts to acceptable levels.

15.3 Recognition Time

i. 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.

ii. 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. Associated Documents

LFR Procedure

GMP Live Facial Recognition PROCEDU

LFR DPIA

Data Protection Impact Assessment DI

College of Policing APP re LFR

Live facial recognition | College of Policing

LFR EIA

Equality Impact Assessment EIA - GMI

LFR Legal mandate

GMP Live Facial Recognition LEGAL M.

LFR Appropriate Processing Notices


LFR - APD General Processing (Final).pdf


LFR - APD Law Enforcement_(Final).pd


PN - Live Facial Recognition (Final).pd

NPIA Capture and Interchange Standard:

npia--capture-and-i
nterchange-standar

FRT Equitability Study:

frt-equitability-study_mar2023.pdf

frt-equitability-stud
y_mar2023.pdf

Data Protection Act 2018

Data Protection Policy v3.0.pdf

Human Rights Act 1998

17. Statutory Compliance & Consultation

17.1 Statutory Compliance

17.1.1 Equality Act (2010)

An Equality Impact Assessment (EIA) has been completed for this policy and can be found **here** [*insert link once* published].

Once the policy and associated EIA have been considered by Chief Officers at Senior Command Team (SCT) meeting, you must complete the below tables.

Date of SCT meeting where Chief Officers reviewed the EIA	*(insert date)*
Summary of Chief Officer discussions/considerations at SCT	(*include brief summary of the evidence they considered, how it was analysed and any discussions)*

State below whether Chief Officers agreed with the EIA, or selected a different outcome:

Outcome	EIA recommended	Chief Officer Decision
Approve – no changes. The policy is robust and the evidence shows no potential for discrimination. All appropriate opportunities to advance equality and foster good relations between groups have been taken.	X	
Approve – subject to amends. Changes are required to remove barriers, better advance equality or mitigate potential effects. This should be done before the policy is implemented.		
Approve – continue with policy. Despite any adverse effect or missed opportunities to advance equality, provided that it does not unlawfully discriminate. The objective justification must be recorded.		
Reject – stop the policy. If there are adverse effects that are not justified and cannot be mitigated, or any unlawful discrimination.		

17.1.2 The UK General Data Protection Regulation (UK GDPR) and Data Protection Act (2018)

Greater Manchester Police has a duty to ensure, so far as is possible, that all staff comply with the provisions of the UK GDPR and the Data Protection Act 2018, particularly relating to their access to, and dissemination of, a wide variety of personal information and intelligence.

This policy has been assessed for compliance issues by the Information Compliance and Records Management Unit (ICRMU) and is considered to be compliant with the legislation as there is a clear lawful basis for the processing of personal data and special category data. It should be read in conjunction with GMP's Data Protection Policy and guidance issued on the Data Protection Intranet pages.

For further information on Data Protection, you should refer to the Force Data Protection Policy or consult the ICRMU by email dataprotection@gmp.police.uk.

17.1.3 Freedom of Information Act (2000)

The Freedom of Information Act 2000 grants a general right of access to all types of recorded information held by public authorities.

As this Policy document contains policing methods, some parts of it may not be suitable for disclosure. Requests for data will be assessed carefully by the Information Compliance and Records Management Unit in consultation with the Policy Owner. All requests will be carefully assessed taking into account the requirement for transparency under the Act, alongside any potential risk of harm in disclosing information into the public domain.

For advice and assistance on the Freedom of Information Act, or any requests for the disclosure of this document should be directed through the Information Compliance and Records Management Unit via the Freedom of Information mailbox.

17.2 Consultation

Consulted	Date	Feedback
Unions:		
Police Federation	16th October	**Consultation Feedback: Live Facial Recognition Policy and Procedure** **GMP Federation (Tim Hanson)** • Section 1 of the Policy - Policy Statement - it states "missing persons deemed at increased risk of harm (as defined by APP)" o The definition needs to be included in this policy to save time in cross referencing to the App. • Section 5.4 (page 15) in the procedure - mentions what forms are needed for a LFR deployment o It could be worth putting this GMP LFR application form at the start of this list (like a checklist for those wanting it) • Section 16 of the Policy & Section 6 of the procedure o This needs to include a link to the college of policing app That's it. Very informative document just a lot of processes hence easier in one document than two. • General o This is a very detailed policy and procedure and contains good information covering all aspects of how LFR would impact on police officers and the public.
GMB	16th October	
UNISON	16th October	

AWP	16th October	
BAPA	16th October	**Black & Asian Police Association (PC Stephen Nalilungwe)** • Reviewed – no comments.
Catholic Police Guild	16th October	
Christian Police Network	16th October	
Disability Support Network	16th October	
Deaf and Hard of Hearing Support Network	16th October	
GMP Pride Network	16th October	
Jewish Police Association	16th October	
Muslim Police Association	16th October	**Muslim Police Association (Tuseef Ahmed)** • Reviewed – no comments.
Sikh Police Association	16th October	
Superintendents' Association	16th October	
Force Crime & Incident Registrar	16th October	**Force Crime and Incident Registrar (CI Helen McCormick)** • Reviewed – no comments.
Health & Safety	16th October	
Human Resources	16th October	**People Branch (Rebecca Smith)** • Reviewed – no comments.
Information Compliance	16th October	
Organisational Learning Hub	16th October	
Legal Services	16th October	