GREATER MANCHESTER POLICE

Deployment of Live Facial Recognition Technology

Procedure

10th Oct 2025

DATE THIS VERSION IMPLEMENTED: October 2025

DATE NEXT REVIEW IS DUE: October 2026

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

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

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

APPROVED BY: ACC Jackson (via Project Board)

GOVERNMENT SECURITY CLASSIFICATION: Official

IS THE PROCEDURE NEW OR REVISED: New

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)	PUBLISHED ON CCOs
1.0	1/11/24	Original version.	Insp Jon Middleton	
1.1	29/09/25	Minor amedments throughout	Ch.Insp Booth	
1.2	10/10/25	Updates re DEI matters in light of current IT solution (Watchlist tool)	Ch.Insp Booth	
1.3	16/10/25	Inclusion of feedback from policy consultation process.	Ch.Insp Booth	

Table of Contents

1. Introduction and Background

This procedure document explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations.

LFR technology uses a live camera feed to scan facial images of a crowd and users 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.

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.

This document should be read in conjunction with GMP's Live Facial Recognition Policy document.

2. Scope

- All operational officers and staff, and their supervisors involved in the planning and deployment of LFR.
- All officers and staff involved in any subsequent investigation resulting from the operational deployment of LFR technology.
- All authorising officers (AOs)
- All officers applying for the deployment of LFR.
- The operational command team for LFR deployment (Gold, Silver and Bronze)
- 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. Roles & Responsibilities

LFR Strategic Lead: Assistant Chief Constable (Crime, Intelligence & Forensics)

Responsible for:

- Supporting the LFR Senior Responsible Officer (SRO) to deliver LFR functionality across GMP effectively through strategic direction.
- Chairing the LFR oversight board to maximise LFR infrastructure and investment.
- Ensuring that GMP has a LFR response that is fit for purpose.

LFR Senior Responsible Officer: Detective Chief Superintendent – Force Intelligence Branch (FIB)

Responsible for:

- Providing performance updates to districts and branches in GMP.
- Maximising the LFR infrastructure and technology in collaboration with districts and branches.
- Ensuring value for money through procurement and partnership with any designated partners surrounding maintenance of LFR infrastructure.
- Reporting to the Home Office any governance surrounding LFR capability or the use of any third party managed service.
- Representing GMP regionally and nationally, or delegating attendance where required.
- Ensuring LFR infrastructure and technology is maximised.
- Harnessing the use of LFR in accordance with GMP's plan on a page.
- Driving improvements through the LFR project board.

LFR Manager: Inspector – ANPR & LFR Manager – Specialist Operations Branch

Responsible for –

- Oversight and governance of operational deployment of overt LFR.
- Training of LFR roles.
- Recording overt LFR performance metrics.

LFR Authorising Officer: Responsible for reviewing the proportionality & necessity of requests to deploy overt LFR, ensuring accountability & legal considerations have been considered.

LFR deployment Gold Commander:
Determines the strategic objectives of the LFR deployment and has overall strategic command of the deployment.

LFR deployment Silver Commander:
Responsible to the Gold commander. Tactical command of the deployment and responsible for tactical implementation. Responsible for ensuring compliance with the AO's Authority and Gold strategy. Responsible for ensuring that use of LFR remains lawful, necessary and

proportionate throughout the deployment having particular regards to the safeguards in place.

LFR deployment Bronze Commander:
Responsible to the Silver commander. Operational command of the deployment and responsible for operational implementation of the Silver commanders tactical plan in line with the Gold strategy. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze.

LFR System engineer:
Responsible for set up of the LFR equipment and optimisation of the FR application to maximise performance. Further information on their roles and responsibilities is contained within section 5.

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. Further information on their roles and responsibilities is contained within section 5.

LFR Engagement Officer:
Responsibility for undertaking the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. Responsible for assisting the public by answering questions and helping them to understand the purpose and nature of the LFR deployment. Further information on their roles and responsibilities is contained within section 5.

4. Terms and Definitions

A full list of terminology relating to this document is contained within the GMP LFR Policy Document section 3.

5. Procedure

5.1 Authority to deploy LFR

i. The authority to deploy LFR in support of a policing operation should be made by an officer not below the rank of Superintendent (the Authorising Officer or AO). Their authorisation should be recorded in writing.

ii. The GMP LFR Application / Written Authority Document recognises that the intelligence case for the use of LFR may give rise to a single Deployment, or a need for a series of Deployments within a time-limited period. Where the GMP LFR Application / Written Authority Document is to be used to authorise a period of up to 7 days during which Deployments may occur, the form provides for a baseline of safeguards to ensure that the need for the Deployment and the currency is the Watchlist continues to be maintained with due oversight.

iii. Should the need to Deploy continue beyond 7 days, a further GMP LFR Application / Written Authority Document must be sought. This approach ensures that the use of LFR is proportionate and kept under review.

iv. Prior to AO authorisation and the Deployment of LFR in public spaces the AO must:

v.

A review of the Force Level Community Impact Assessment and Equality Impact Assessment should be completed and documented. Where necessary a bespoke local CIA ~~and EIA~~ 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.

- A GMP officer of Command rank (ACC rank or above or Police Staff equivalent) must be briefed on the proposed deployment by the AO.

vi. Whilst the senior officer does 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. This affords NPCC the opportunity to veto the deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

vii. If they authorise the deployment the AO must ensure that the following are briefed on the proposed deployment:

- An officer of the rank of Superintendent or above for the relevant District/s (if not the same as the AO) is aware of the proposed deployment, and
- The Office of the Deputy Mayor for Stronger & Safer Communities.
- The Duty ACC (via DMM/Force Operations Centre).
- Criminal Justice & Custody Branch

viii. Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable.

5.1.1 Role of AO

The AO must:-

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

b) satisfy themself that the deployment complies with GMP LFR policy and impact assessments, or is otherwise authorised; and

c) from a Human Rights Act 1998 perspective, articulate

(i) how and why the Deployment is necessary (and not just desirable), and
(ii) is proportionate to achieve the legitimate aim of the Deployment; and

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

e) articulate that the deployment is necessary on at least one of the following grounds (the ground(s) to be confirmed by AO):

i. Necessary for GMP's lawful policing purposes for reasons of substantial public interest; and / or

ii. Necessary for the administration of justice; and / or

iii. Necessary for the safeguarding of children and/or of individuals at risk; and

iv. Necessary notwithstanding any expectations people may have pursuant to their Article 8 human rights regarding the respect of private and family life, as well as other human rights considered by the AO.

f) articulate that they have given regard to the safeguards proposed for the Deployment and the safeguards contained within the GMP LFR documents, and considers that the deployment in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the Data Protection Act 2018 and UK GDPR; and

g) articulate that they are satisfied that all reasonable steps have been taken to ensure that the composition of the Watchlist complies with GMP LFR documents, including the legality, necessity and proportionality criteria; and

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

i) that all police officers / staff engaged in the deployment must have received LFR training as per the GMP LFR documents; and

j) satisfy themselves that the deployment is proportionate with the benefits anticipated from the use of LFR outweighing the concerns and impacts there may be in relation to people's human rights and rights relating to equalities; and

j) satisfy themselves that the control measures in the Data Protection Impact Assessment, Community Impact Assessment, and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigation for the deployment.

k) determine the minimum Threshold setting to be utilised during the Deployment. Ordinarily this setting will be equal to or above the value where no FRT System bias is detected (0.64 with the current FRT algorithm). The Threshold value may be lowered based on the intelligence case with a full rationale detailed in the GMP LFR Application / Written Authority Document.

5.1.2 Urgent cases

i. Situations where the need for an authorisation to be granted urgently may include:-

   a) an imminent threat-to-life or of serious harm to people or property; and / or

   b) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which supports the urgency of action.

ii. Should a further law enforcement purpose be identified after the AO has issued their authority for an LFR Deployment, processing in respect of the law enforcement purpose is not permissible unless the AO grants a further authority for it. Such authority would consider the lawfulness, strict necessity and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.

5.2 Date, time, duration & location of deployment

i. The AO should define the date, time, location and duration the deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the deployment.

5.2.1 Considerations relevant to a LFR Deployment location

ii. The intelligence case, policing purpose to include a person on a Watchlist, Community Impact Assessment and the environmental factors relevant to a potential deployment location will substantially inform the potential locations for LFR Deployments.

iii. Deployment locations will be determined by there being reasonable grounds to suspect that the proposed deployment location is one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any selected deployment location should be recorded and be capable of being considered and evaluated by an objective third person.

iv. The selection of a particular deployment location may further be supported by:

a. policing information or intelligence about a proposed Deployment location including if there is an increased public safety risk and/or need to provide public reassurance at the location; *and*

b. the ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so.

v. When reviewing a potential Deployment location, AOs must also consider:

a. Those who are likely to pass the LFR system and the reasonable expectations of privacy they may have as a whole at that location (some places by their nature attract greater privacy expectations than others)

b. The number of cameras used by the LFR System to ensure the size and scale of the deployment enables those on a watchlist to be effectively located without disproportionately processing biometric data.

c. If a proposed deployment location attracts particular concerns by reference to those expected to be at a particular location (for example hospitals, places of worship, centres for legal advice, polling stations, places of education, lawful assemblies) there may have a greater expectation of privacy and/or people may feel less able to express their views or otherwise attend the location area.

vi. Where it is practicable to identify a person of being responsible for a proposed deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate.

vii. Where privacy or other human rights considerations are identified in relation to a particular deployment, the AO needs to consider the necessity to deploy LFR to that particular location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is necessary (with the processing of data at that site being strictly necessary), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR System against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.

5.2.2 Measures during an LFR deployment

i. Save in exceptional operational cases where doing so would undermine objectives or operational imperative of the deployment (for example, in cases of urgency or where it would compromise other policing tactics) the public should be notified of LFR deployments in advance.

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

iii. In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any Deployment is overt, the objectives for the deployment and its use a policing tactic will also be relevant if the policing need to deploy is to be realised. For example, unduly extensive signage may undermine the effectiveness of a Deployment seeking to locate persistently outstanding offenders. By comparison a Deployment seeking to protect a site or particular event may merit multiple levels of signs and the proactive distribution of leaflets to deter criminality.

iv. If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of a policing power. GMP staff deployed must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.

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

5.3 Watchlist generation & criteria for inclusion of an image on a watchlist

5.3.1 Safeguards relevant to all Watchlists

The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria stipulated in this GMP LFR procedure and be specific to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:

Requirement	Rationale
Intelligence: Watchlists must be driven by a policing need and based on the intelligence case. The intelligence case must be current and reviewed before each Deployment.	This intelligence-driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR deployment
Images sources: Watchlists must only contain images lawfully held by police with consideration also being given as to: i) the legal basis under which the image has been acquired; and ii) the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.	This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance. Additionally policing has a responsibility to avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image: i) is of a person intended for inclusion on a given Watchlist; and; ii) is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator).	This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The GMP SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.

Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment	This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours
Watchlist design: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated.

5.3.2 Additional safeguards relating to protected characteristics

i. Following on from the Bridges case, in December 2020 the then Surveillance Camera Commissioner (SCC) published the best practice guidance document 'Facing the Camera'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist.

ii. Any controls, mitigations and processes identified by GMP in this document reflect GMP LFR system's performance and GMP's particular use cases for LFR.

iii. GMP has confidence in the LFR System's performance, particularly in relation to gender, age and race.

iv. GMP recognises that regardless of performance considerations, it should take particular care when considering and publishing details relating to age including the protection of children – particularly the very young, persons with disabilities and those who have and/or are undertaking a gender reassignment. This is because:

   a. There may be different privacy expectations around the use of LFR for persons with these protected characteristics and that these can be particularly relevant in relation to these people given their potential vulnerability.

   b. GMP recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic. 6.6

v. GMP recognises the risk factors regarding the inclusion of persons under 18 and those under 13 years of age. Where watchlist requirements suggest that young persons are to be included then this needs to be highlighted to the authorising officer (AO) such that due consideration can be given to the proportionality of that and what additional safeguards may be necessary.

vi. GMP will record all engagements with subjects identified by LFR and collate associated DEI data to meet DEI reporting requirements.

vii. GMP is committed to the development of its watchlist creation tool and will work with ITDD colleagues to ensure that further iterations of the tool allow for the breakdown and capture of other protected characteristics.

viii. Safeguards regarding composition - the following outlines further, specific safeguards that apply to the composition of the Watchlist:

	Age – Under 18	Age – Under 13	Disability	Gender Reassignment
Circumstances				
	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 18-years-old	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old[7]	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment
Safeguards				
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with LFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Watchlist Images		There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.		
Legal Advice		Specific advice must be sought from Legal Services and the GMP LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		
Technical Advice		Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.		
	Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be blocked from the camera's line of sight.	Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.		

5.3.3 Police originated images that may be included on a watchlist

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

   a. wanted by the courts; and/or

   b. suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or

   c. subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment; and/or

   d. missing persons deemed increased risk; and/or

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

   f. who are a victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual and that individual themselves would fall within paragraphs (a) – (f).

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

5.3.4 Non-police originated sources of Watchlist imagery

i. Where it is viable to do so without unduly impacting on the performance of the LFR System, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by GMP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.

ii. Non-police originated images are images which have not been taken by law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three ‘layers of intrusiveness.

Assessing non-police originated sources of watchlist imagery		
		
Layer A	Layer B	Layer C
Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including: • where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage; • where the police have obtained the image as a result of a lawful power of search or seizure; • data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.	Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject, including any imagery obtained pursuant to: • the Regulation of Investigatory Powers Act 2000; and • the Investigatory Powers Act 2016, where the ability of relevant bodies to obtain such images is further supported and can be anticipated by reference to published Codes of Practice.	Non-police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received. To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.

iii) Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular which layer of intrusiveness the image is attributable to and the factors at 5.3.3 above.

iv) The types of non-police originated images that may be deemed appropriate for inclusion within an LFR Watchlist are of people are the same as per section 5.3.3 i) above.

5.3.5 Persons who may be included on a watchlist – definitions:

"Wanted by the courts" - This term includes those with outstanding arrest warrants or who are otherwise required by the courts. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended.

"Missing persons deemed increased risk." - This term is as per the College of Policing definition of medium risk (or above) that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.

"Presenting a risk of harm" - Mitigating the risk of harm to themselves or to others will need to have a legal basis for action under a policing common law power. 'Harm' can include a risk of harm arising in relation to a person's welfare and/or a financial harm including as a result of fraud or other dishonesty. It can also include 'Harm' in the context of posing a risk to national security.

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

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

The applicant would also have to demonstrate the proportionality of any inclusion on a Watchlist. This would include considering:

a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
b) the importance of locating the person or people sought with reference to the threat, harm and which the addition to the Watchlist addresses;
c) whether the significance of the threat, harm and risk identified, which inclusion on the watchlist would address outweighs any expectations of privacy.

"Victim of an offence, or a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual."

This criteria includes a victim, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within paragraphs section 5.33 (a) – (e) of the categories that may be deemed appropriate for inclusion within an LFR Watchlist.

The threshold for any Watchlist inclusion is high and the use of the category will be by exception; the necessity for inclusion must be based on a specific intelligence-case with the

need for the inclusion on a watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to able to demonstrate to the AO's satisfaction:

a) why the inclusion of each victim, person reasonably suspected of having information, or close associate is necessary to help locate the person who is wanted by the courts and/or the police; and/or

b) why locating each victim, person reasonably suspected of having information, or close associate person is necessary to advance the policing investigation; and/or

c) why locating each victim, person reasonably suspected of having information, or close associate is necessary to ensure their safety and/or the safety of others.

The applicant would also have to demonstrate the proportionality of any inclusion on a watchlist. This would include considering:

a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and

b) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;

c) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any inclusion on the watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others.

5.4 GMP LFR documentation required for deployments

i. For each authorised LFR deployment, the following documents must be reviewed to see if they are appropriate and relevant for that deployment. If not, then a new amended version should be created to cover that deployment.

    a) Data Protection Impact Assessment
    b) Equality Impact Assessment
    c) Community Impact Assessment
    d) Surveillance Camera Commissioner's Self-Assessment

The most recent copies of the documentation required for an LFR application can be found on the LFR Intranet site, under Specialist Operations.

5.5 Management of risk & resourcing

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

The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.

Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to alerts and to meet the law enforcement purpose of the LFR deployment.

~~LFR System Engineers will be deployed to support LFR deployments and will come with suitable vehicles where required.~~ LFR System Engineers may be deployed to support LFR deployments.

All GMP officers and staff deployed on LFR Deployments must be in date with first aid and PPST training requirements. All GMP officers and staff involved in an LFR deployment must receive LFR training prior to being deployment relevant to their roles on that deployment.

5.6 Planning & booking

Applications for GMP LFR deployments will initially be assessed by the FIB, in line with the agreed tasking and coordination process through FTTCG. The operational LFR team will provide expert advice to applicants in submitting paperwork and will work with districts and branches once authority has been provided.

GMP's LFR team will securely maintain all records relating to LFR deployments, carry out recce's and planning in advance of deployments and maintain a record of planned deployment dates/time & locations for the NW regional LFR capability.

5.7 Operational Roles

5.7.1 LFR command team

LFR deployments must be supported with a clear command structure which is agreed as part of the application process. For larger events or specific operations a specific GSB (Gold, Silver & Bronze) structure may be put in place.

For smaller deployments the operational LFR team will require a district / branch Gold who will provide oversight and the final responsibility that the use of LFR remains, lawful, necessary and proportionate. They will also ensure that the duty ACC is aware of the deployment

The operational LFR team will be provided with district / branch contacts prior to the deployment in order to ensure adequate resources are available to brief and run the operation itself.

i. Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze may be substituted for alternative command team terminology or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

5.7.2 LFR Operator

i. LFR Operators receive detailed training prior to being deployed operationally. Their role is to monitor and assess application Alerts, before working with LFR Engagement Officers (as necessary) to decide whether an Engagement is required.

ii. The LFR Operator must log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR System performance to the command team.

iii. The LFR Operator's log should include:- a) the LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; and b) what decision was taken regarding whether to Engage a member of the public or not; and c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

5.7.3 LFR Engagement Officer

i. LFR Engagement Officers must have an understanding of the LFR application, how it performs, and what effect Subject, System, and Environmental Factors might have. These officers must receive a full operational briefing prior to deployment. These officers may be deployed in uniform or plain clothes.

ii. When conducting an Engagement, LFR Engagement Officers must ensure that they do so lawfully, and in an appropriate and proportionate manner. Officers must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject of an Engagement, should be supplied with an LFR information leaflet.

iii. The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.

iv. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own `reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take.

v. When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal.

vi. Whilst officers must exercise their own discretion when using their powers of arrest and detention, GMP policy is that an LFR application-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is

reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

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

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

ix. Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so.

5.7.4 LFR System Engineer

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

5.8 Post-deployment

i. Following each LFR deployment, the Silver Commander must ensure that a post deployment evaluation is completed which is updated in the deployment Record. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both qualitative and quantitative in nature.

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

iii. The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (including what methods were used to obtain them):

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

b. total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR application was able to generate a Template from them); and

c. total number of LFR application-generated Alerts; and

d. total number of Alerts that do not result in an Engagement; and

e. total number of Alerts where a decision was taken to Engage an individual; and

f. total number of Alerts that are confirmed as true alert (the individual is who the LFR application suggests are); and

g. total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and

h. total number of correct Alerts that result in an Engagement that do not require any further police action; and

i. outcome of each case where police action is instigated following an Alert; and

j. number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome; and

k. the threshold setting for the deployment

6. Associated Documents

LFR Policy

GMP Live Facial Recognition POLICY V

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).p

PN - Live Facial Recognition (Final).pd

NPIA Capture and Interchange Standard:

npia--capture-and-interchange-standar

FRT Equitability Study:

frt-equitability-study_mar2023.pdf

Data Protection Act 2018
data protection policy v3.0.pdf
Human Rights Act 1998

7. Statutory Compliance & Consultation

7.1 Statutory Compliance

7.1.1 Equality Act (2010)

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

Once the procedure and associated EIA have been considered by the relevant Decision Maker, you must complete the tables below. In the majority of cases, the Decision Maker for a procedure will be the Branch Head/Chief Superintendent, however it may go to Chief Officers at Senior Command Team (SCT) meeting in exceptional circumstances. The SPP Team will advise on this.

Date that Decision Maker reviewed the EIA	*(insert date)*
Summary of Decision Maker's discussions/considerations	(*include brief summary of the evidence they considered, how it was analysed and any discussions)*

State below whether the Decision Maker agreed with the EIA, or selected a different outcome:

Outcome	EIA recommended	Decision Maker
Approve – no changes. The procedure 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 procedure is implemented.		
Approve – continue with procedure. 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 procedure. If there are adverse effects that are not justified and cannot be mitigated, or any unlawful discrimination.		

7.1.2 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 procedure 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.

7.1.3 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 Procedure 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 Procedure 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.

7.2 Consultation

Consulted	Date	Feedback
Unions:		
Police Federation	October 2025	Please refer to accompanying feedback for the Policy document.
GMB		
UNISON		
AWP		
BAPA		
Catholic Police Guild		
Christian Police Network		
Disability Support Network		
dDeaf and Hard of Hearing Support Network		
GMP Pride Network		
Jewish Police Association		
Muslim Police Association		
Sikh Police Association		
Superintendents' Association		
Force Crime & Incident Registrar		
Health & Safety		
Human Resources		
Information Compliance		
Organisational Learning Hub		
Legal Services		

8. Appendices

None.