Merseyside Police

Live Facial Recognition (LFR)

Standard Operating Procedure

OFFICIAL

Publication Scheme	**Government Security Classification Scheme (GSCS):** **Official.** ***The level of security classification indicates the sensitivity of information. The Policy Author will determine the classification of either OFFICIAL or OFFICIAL- SENSITIVE. A handling rule may also be added for example OFFICIAL-SENSITIVE-For Police Eyes Only.*** **Standard Operating Procedure on External Force Website?** **Yes – Standard Operating Procedure**
Department of Origin	***Matrix Force Operations***
Policy Holder	***Chief Supt Zoe Thornton***
Policy Author	***Sgt Chris Hilton***
Related Information **(Insert hyperlinks to related information)**	
This Version	**1**
Date Created / Modified	**03/12/2025**

Review By *(3 years)*	**03/12/2028**

Contents

1 Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations. Compliance with the SOP will help ensure correct use of this policing tool. This SOP sets out mandatory steps for planning, authorisation, deployment, and review of LFR technology. It ensures deployments are lawful, necessary, proportionate, transparent, and consistent with national guidance and best practice.

2 Application and Scope

2.1 All Merseyside Police officers and police staff, including members of the extended police family, volunteers, and those working under contract to the Chief Constable, must be aware of and comply with all relevant Merseyside Police policy and associated procedures when planning for or using Live Facial Recognition (LFR) technology.

2.2 This SOP applies in particular to officers and staff in the following roles:
a) All operational officers and police staff, both uniformed and detective, and their supervisors involved in the planning and deployment of LFR technology; and
b) All police officers and police staff involved in any subsequent investigation resulting from the operational deployment of LFR technology; and
c) All Authorising Officers (AO); and
d) The operational command team for any LFR deployment (Gold, Silver, and Bronze Commanders); and
e) LFR Operators, LFR Engagement Officers, and LFR System Engineers.

Note: This list is not exhaustive. Any individual who has a role in the planning, deployment, or post-deployment processes of LFR must comply with this SOP.

3. Roles & Responsibilities

Authorising Officer (AO)

- Must be Supt or above.
- Reviews and approves LFR applications.
- Completes and signs the Written Authority Document (WAD).
- Confirms compliance with policy, DPIA, EIA, proportionality, and safeguards.
- Provides ongoing authority if deployment exceeds 24 hours.

Applicant

- Must be Ch/Insp or above, or have Ch/Insp or above as sponsor.
- Complete and submit the LFR application accurately.
- Review CIA/EIA for local concerns and record mitigation.
- Plan resourcing for engagement officers.
- Prepare pre deployment community engagement measures

Silver Commander

- Maintains tactical oversight of deployment.
- Ensures deployment remains within AO authority.
- Coordinates operational resources and supervises LFR Bronze.
- Typically LPA Command Team or Event Silver

LFR Bronze

- Oversees LFR deployment site
- Ensure signage is displayed and community awareness measures are implemented.
- Manages deployment logs.
- Uploads and validates watchlists.
- Supervises operators and engagement officers.
- Brief Engagement Officers
- Must complete NPCC LFR training before participation.

LFR Operators

- Operate LFR equipment in vans and at deployment sites.
- Monitor live feeds and system alerts.
- Verify alerts manually before intervention.
- Record all alerts, matches, and interventions in deployment log.
- Must complete NPCC LFR training before participation.

Engagement Officers

- Provide visible presence at deployment sites.
- Answer public queries and explain purpose, safeguards, and rights.
- record all public interactions in deployment log.
- Act on alerts by stopping suspect and dealing with them appropriately
- Must justify any policing powers used following an alert.

4 Written LFR Application

4.1 Applicant Guidance

Before completing the form, read these instructions carefully. They explain why each section matters and what information you must provide.

4.2 Section 1 [A]: Applicant Details

This section establishes accountability for the application and ensures that oversight is maintained throughout the deployment. The Authorising Officer needs to know who is responsible for submitting the request and who will provide tactical oversight during the operation. This information is essential for legal compliance and operational governance.

Begin by providing your full name, rank, collar number, role, and contact details. If you are below the rank of Chief Inspector, you must include a sponsor who holds the rank of Chief Inspector or above. This requirement ensures that the application has appropriate supervisory endorsement and that the decision to deploy LFR is supported at the right level of command.

You must also include details of the Silver Commander who will maintain tactical oversight during the deployment. Provide their rank, name, collar number, and contact number. The Silver Commander must be contactable throughout the operation and is responsible for ensuring that the deployment remains within the authorised scope and complies with all safeguards. The Silver Commander for the deployment will typically be a Chief Inspector or above from the command team of the Local Policing Area (LPA) where the deployment occurs, or the Silver Public Order Policing (POPS) Commander for an event.

4.3 Section 1 [B]: Deployment Type

In this section, you need to define the operational context for using LFR. Start by explaining which category applies to your operation and why:

- Proactive deployments involve the planned use of Live Facial Recognition technology, with the primary objective of locating individuals who are wanted by the police or pose a risk to public safety. These deployments are strategically positioned identified area experience criminality where there is a higher likelihood of encountering persons of interest such as major shopping districts, transport hubs, or event venues.
- Event-specific deployments are linked to scheduled events such as football matches, concerts, or public gatherings where there are heightened public safety concerns.
- Incident or intelligence-led deployments occur in response to specific intelligence or an ongoing investigation. These are typically urgent and require a clear explanation of the intelligence source and why immediate action is necessary.

You must also state the number of LFR vans requested—usually one or two—and ensure that this aligns with the operational objectives and the scale of the deployment. For example, a large

public event may justify two vans, while a targeted intelligence-led operation may only require one.

4.3 Section 1 [C]: In□ormation and Intelligence Case

Start by summarising the relevant crime trends that underpin the need for deployment. These should be drawn from documents produced by Corporate Support and Development (CSD) and supported by Delphi analysis, which provides an evidence-based picture of crime patterns and hotspots. For example, you might reference an increase in knife-related assaults in a specific area or a series of burglaries linked to organised crime groups.

Next, detail the intelligence case. Intelligence must come from documents produced by the Force Intelligence Bureau (FIB) and should include consultation with FIB support to ensure accuracy and currency. This step is essential because it confirms that the intelligence is reliable and up to date. Explain how this intelligence links directly to the operational objectives—for instance, identifying high-risk offenders who are known to frequent the deployment area.

You should also attach supporting documents such as maps, crime reports, or intelligence summaries to strengthen your case. These attachments help the AO understand the context and validate your rationale. Finally, confirm that the intelligence has been reviewed and validated by the relevant unit, ensuring compliance with policy and safeguarding against arbitrary use of LFR.

The Authorising Officer will rely on this information to determine whether the deployment is necessary and proportionate under the Human Rights Act and the Data Protection Act. It is not enough to state that LFR will “help prevent crime”—you must demonstrate a clear policing purpose supported by validated information and intelligence.

4.4 Section 1 [D]: Objectives, Legitimate Aim & Legal Basis

Start by explaining the purpose of the deployment in simple terms. What are you trying to achieve? For example, you might want to find people who are wanted on warrant, help protect vulnerable individuals such as missing children or prevent serious crime during a high-risk event.

Next, set out the legitimate policing aims that support this purpose. These should link to recognised policing objectives, such as keeping the public safe, preventing crime or disorder, or protecting national security. This shows that the deployment is not arbitrary but based on clear operational needs and intelligence.

Finally, confirm the legal basis for using LFR under the Data Protection Act 2018 and UK GDPR. This means showing that the deployment is necessary for law enforcement purposes, serves a substantial public interest, or is required to safeguard individuals at risk.

When completing this section, you are setting out the foundation for why the deployment of LFR is lawful and justified. The Authorising Officer needs to understand not only what you intend to achieve but also how this aligns with policing powers and legal frameworks.

4.5 Section 1 [E]: Location(s)

Start by clearly stating the proposed location or locations for the deployment. Explain why these areas have been selected and how they support the policing objectives outlined earlier. For example, you might reference crime trends or intelligence indicating that high-risk individuals frequent these locations, or that the area is a hotspot for serious offences.

You must also confirm that the Community Impact Assessment (CIA**)** has been reviewed in relation to the proposed location. This review should identify any local sensitivities, such as cultural or religious considerations, and outline steps taken to mitigate potential concerns. If additional community impact issues have been identified beyond those in the standard CIA, describe them here and attach any supplementary assessments.

Mitigation measures should be practical and proportionate. These may include adjusting the deployment footprint to avoid areas of elevated privacy, such as hospitals, schools, or places of worship, or implementing enhanced signage and public engagement to maintain transparency.

The Authorising Officer needs to understand why the chosen location is operationally justified and how risks to privacy and community confidence will be mitigated.

4.6 Section 1 [F]: Dates and Times

Begin by specifying the proposed authorisation period. This should not exceed 14 days per application**.** If the operational requirement extends beyond this, a new application and authorisation will be required. Clearly state the start and end dates and times for the deployment, and if multiple deployments are planned within the authorisation period, list each date and time individually.

If the deployment will last longer than 24 hours**,** additional safeguards apply. You must confirm that the watchlist will be refreshed daily to ensure its currency, that the intelligence case will be reconfirmed each day, and that the LFR Operator will log these checks. The Authorising Officer must also be consulted daily to confirm that the basis for deployment remains valid.

The Authorising Officer must be able to confirm that the proposed duration is proportionate to the policing need and that safeguards are in place for extended deployments.

4.7 Section 1 [G]: Watchlist Selection

Start by identifying which watchlist you want to include in your deployment, such as Counter Terrorism, Wanted on Warrant, Missing Persons, or event-specific lists, and provide a clear justification for each. Explain why the watchlists are relevant and how their inclusion supports the operational objectives.

The Authorising Officer must be satisfied that each watchlist included meets the criteria set out in policy and that the inclusion is necessary for the policing purpose.

You must also confirm the image levels and provenance for all watchlist entries. Image levels indicate the privacy expectation associated with the source of the image:

- **Level 1 – Lowest Privacy Expectation:**
  Police-originated images taken in compliant circumstances or with consent.
  Examples: Custody photographs, images provided by a parent for a missing child, BWV footage where the subject is cooperative.
- **Level 2 – Low Privacy Expectation:**
  Police-originated images taken in non-compliant circumstances but overt.
  Examples: Non-compliant custody photo, overt CCTV, BWV where the subject is non-cooperative.
- **Level 3 – Moderate Privacy Expectation:**
  Non-police images where public would expect law enforcement access.
  Examples: Images from public appeals, local authority CCTV, open-source information, employer-provided photo.
- **Level 4 – Elevated Privacy Concerns:**
  Images obtained covertly under lawful powers.
  Examples: RIPA/IPA imagery, images from sensitive locations such as hospitals or schools.
- **Level 5 – Highest Privacy Expectation:**
  Non-police images where sharing with police was not anticipated.
  Examples: Images given to a private company for a specific purpose (e.g., business promoting privacy).

If you propose to use Level 4 or Level 5 images, you must provide a detailed legal justification and reference the authority under which these images were obtained (e.g., RIPA or IPA warrant). Include the warrant number, authorising officer, and date of authorisation. Attach supporting documentation where necessary.

4.8 Section 1 [H]: Algorithm Threshold

Under Merseyside policy and NPCC guidance, the default threshold is 0.64, when using the NEC NeoFace system. This value has been selected because it represents the point at which the system performs accurately without introducing bias or disproportionate intrusion. If you intend to use a different threshold, you must provide a clear and detailed rationale. This should explain why the variation is necessary, how it relates to the intelligence case, and what safeguards will be in place to mitigate any increased risk of false alerts or privacy impact.

The algorithm threshold determines the confidence level at which the system will generate an alert. Setting this value correctly is essential to avoid unnecessary interventions while ensuring operational effectiveness.

4.9 Section 1 [I]: Legality, Necessity & Proportionality

Begin by explaining why the deployment is essential to achieving a legitimate policing aim, such as preventing serious harm or locating high-risk offenders, and link this directly to the intelligence case provided earlier.

Next, confirm that you have considered less intrusive methods and explain why they are insufficient. This shows compliance with the principle of proportionality under the Human Rights Act and ensures that LFR is only used when alternatives cannot achieve the same policing objective.

You should then describe how the deployment will minimise intrusion and protect individual rights. This includes limiting the deployment footprint, reducing the duration, avoiding sensitive locations such as hospitals or places of worship, and ensuring transparency through public engagement. These measures demonstrate that the deployment strikes a fair balance between policing objectives and the rights of individuals.

Finally, outline how you will inform the public about the deployment. Planned awareness measures should include signage at entry points, updates on official channels, and engagement officers on site. This transparency supports compliance with both the Human Rights Act and Data Protection Act by ensuring individuals are aware of the processing of their personal data.

4.10 Section 1 [J]: Human Rights Considerations

Begin by addressing Article 8, which concerns the right to respect for private and family life. Explain whether the deployment involves areas of elevated privacy, such as hospitals, schools, or places of worship, and describe what measures you will take to minimise intrusion. Then consider Articles 9 to 11, which relate to freedom of thought, conscience, religion, expression, and assembly. If the deployment is near a protest, religious gathering, or public meeting, outline how you will ensure these rights are not disproportionately affected. Article 14 requires you to consider whether the deployment or watchlist composition could have a discriminatory impact on protected groups and explain how this will be mitigated.

Your narrative should show that you have reviewed these rights carefully and applied safeguards to strike a fair balance between policing objectives and individual freedoms. This includes avoiding sensitive locations where possible, limiting the duration and scope of the deployment, and ensuring transparency through public engagement and awareness measures. You must show that you have considered the potential impact on Articles 8 to 14 and taken steps to mitigate any risks.

5 Written Authorisation Document (WAD)

5.1 Authorising Officer Review and Authorisation

Once the application for an LFR deployment is complete, the Authorising Officer (AO) must review it thoroughly to confirm compliance with the Merseyside Polices LFR Policy, Data Protection Impact Assessment (DPIA), the Equality Impact Assessment (EIA), Merseyside Police LFR Legal Mandate, and LFR Community Impact Assessment. The AO must check that proportionality has been properly assessed and that appropriate safeguards are in place to minimise intrusion and protect individual rights.

The AO must confirm the legal basis for the deployment, which includes reliance on common law policing powers, such as preventing and detecting crime, protecting life, and bringing offenders to justice and Section 64A of the Police and Criminal Evidence Act 1984. Compliance with Article 8 of the Human Rights Act is essential; any interference with privacy must be lawful, pursue a legitimate aim, and be necessary and proportionate. The AO must clearly articulate the operational purpose and demonstrate how LFR supports a legitimate policing aim, such as public safety or protecting vulnerable individuals. This decision must be supported by an intelligence case and show that LFR is necessary rather than merely desirable. Alternative methods considered and discounted should be recorded.

Watchlist composition must also be reviewed to ensure it meets necessity and proportionality tests, is based on objective and lawful criteria, and is tailored to the specific deployment. The AO must approve any non-police-originated images after assessing privacy implications and confirm that the Watchlist will be deleted within 24 hours of the deployment's conclusion.

Privacy and equality considerations must be addressed. The AO should assess the deployment location for privacy expectations and record mitigations to minimise impact, such as signage and limiting the zone of recognition. Potential impacts on Articles 9, 10, and 11, covering freedom of religion, expression, and assembly, must also be considered. Compliance with the Equality Act 2010 and the Public Sector Equality Duty must be ensured, including confirmation that officers have been briefed on unconscious bias and that algorithm performance has been independently tested for demographic fairness.

Data protection compliance is critical. The AO must confirm that biometric data processing is strictly necessary for law enforcement purposes under the Data Protection Act 2018 and that a current DPIA is in place. Retention and deletion standards must be observed, with biometric data and Watchlists deleted within 24 hours and CCTV footage within 31 days.

After completing this review, the AO must record their decision by signing and dating the Written Authority Document (WAD). This signature confirms that the deployment is lawful, necessary, and proportionate, and that all required considerations have been addressed. Deployment cannot proceed without written authority from the AO. This step provides formal approval and ensures that the operation is subject to proper oversight before any activity takes place.

6 Watchlist Creation and Handling Validation

6.1 Watchlist Upload and Trans□er to LFR System

The watchlist must be created and managed in a way that ensures accuracy, security, and compliance with policy. Only specified and trained LFR officers are authorised to handle watchlists.

At the start of each deployment, the LFR Officer must only upload the authorised watchlists authorised by the designated Authorising Officer. This transfer must strictly follow the approved process and use only preapproved pen drives which uses AES-CBC 256-bit full disk hardware encryption to maintain data security. The encrypted pen drives will be allocated to the LFR team and, when not in use, must be stored securely in the Matrix Force Operations vehicle key cabinet.

All pen drives used for LFR deployments will be subject to strict access and security controls. Passwords for encrypted pen drives will be stored securely by the LFR Team in accordance with organisational policy and will not be shared openly. A unique password will be assigned to each pen drive to maintain data integrity and prevent unauthorised access.

The watchlist data will be securely stored in the folder S:\Matrix Force Operations\LFT Watchlists, which is configured with read-only access for the LFR team. Each day between 06:00 and 07:00 hours, the watchlists in this location will automatically refresh to ensure they remain current. Once the approved watchlist is available, the LFR team must copy it from the secure folder and transfer it onto the designated encrypted pen drive. This step ensures that the correct and most up-to-date watchlist is used for operational purposes. The transfer process must be recorded in the deployment log, including the date and time of transfer and the officer responsible,

The LFR Officer must only connect the pen drive to the LFR system running NEC NeoFace. The officer then accesses the authorised watchlist stored on the pen drive and uploads it to the system using the approved process.

Once the transfer is complete, the pen drive must be placed in a locked box within the LFR van. This ensures physical security and prevents unauthorised access during the deployment. The location, time watchlist was uploaded and storage should be recorded in the deployment log, and the pen drive must remain secured until the end of the operation.

6.2 Watchlist Deletion

At the end of the deployment, it is the responsibility of the LFR Officer to delete the watchlist from both the LFR system and the pen drive immediately or soon as is possible. This action must be recorded in the deployment record and the cancellations report, including the time, date, and the name of the officer who performed the deletion. Once the deletion is complete and the officer has returned to the station, the pen drive must be placed back in the secure cabinet located in the Matrix Force Operations vehicle key storage cabinet.

6.3 Watchlist Regeneration 24hours +

For deployments lasting more than 24 hours, the watchlist must be regenerated and re-uploaded daily to maintain currency. At the same time, reconfirm the intelligence case and record this validation in the deployment log. If the intelligence is no longer valid, the deployment must be suspended immediately.

7 Pre Deployment Actions

7.1 Resource Booking

Once authorisation is granted, the next step is to secure the necessary LFR resources. Merseyside Police does not own LFR vans; the regional LFR asset is managed by Greater Manchester Police (GMP). To book the van, contact the GMP LFR team via lfr@gmp.com and also notify the Northwest Regional Information Coordination Centre (NWRICC) at NW.RICC@gmp.police.uk. The booking request must include deployment dates, times, and location.

For staffing, a guide is that one LFR van requires two trained LFR operators to manage the system and six to eight engagement officers to handle public interaction, address concerns, and make interventions following alerts. In addition, assign a Bronze Officer to oversee the deployment on the ground and a Silver Commander to provide tactical oversight. All resourcing must be coordinated with the Force Resource Unit (FRU), and Smartforce Duties should be updated with Op Linksight as the operation name.

7.2 Site Assessment

Before deployment, LFR operators are to carry out a site assessment to confirm that the proposed location of the LFR Vans. The location should provide clear camera coverage and sufficient pedestrian traffic to meet the objectives outlined in the intelligence case.

The LFR operator must review the deployment application and any associated comments, including those relating to the Community Impact Assessment (CIA) and Equality Impact Assessment (EIA). This review should identify any location-specific concerns and consider whether the deployment could affect local sensitivities or raise community issues. Where such risks exist, the operator must document any mitigations required to address them.

The operator must also identify areas of elevated privacy within or near the deployment zone, such as hospitals, schools, or places of worship. Where these are present, adjustments should be made to the deployment footprint or camera positioning to minimise intrusion and ensure compliance with human rights and data protection obligations.

As part of the site assessment, conduct a risk assessment to ensure the safety of officers and staff who will be deployed. This should include evaluating potential hazards and environmental factors. Record any control measures implemented to mitigate these risks.

Finally, document all findings in the deployment log. This should include confirmation of suitability, any adjustments made, privacy mitigations, and the outcome of the risk assessment.

7.3 Community Awareness

They LFR applicant must inform local community representatives and relevant stakeholders about the planned deployment. This may include local councillors, community groups, or business forums, depending on the location and context. Early engagement supports trust and addresses potential concerns before the operation begins. The LFR team will ensure the website is updated with the deployment dates and location.

8 Deployment Phase

8.1 Oversight

Throughout the deployment, the Silver Commander maintains overall tactical oversight, ensuring that the operation remains lawful, proportionate, and aligned with the authorised plan. Typically, this role will be filled by a member of the command team from the Local Policing Area (LPA) where the deployment is taking place. For Public Order Public Safety (POPS) operations or major events, the designated Silver Commander for the event will assume responsibility for oversight to ensure consistency with the wider policing strategy and operational objectives. LFR Bronze will be trained LFR operators and are responsible for managing the deployment log and confirming that all checks and reconfirmations are completed as required.

8.2 Operational Briefing

Before deployment begins, LFR officers will conduct a comprehensive briefing for all staff involved. The briefing should cover the operational objectives and explain how LFR technology works. Roles and Responsibilities will be allocated and explained during the briefing.

All officers are reminded that alerts generated by the LFR system are not identifications. They are prompts for further consideration, and officers must exercise discretion before taking any action. This reinforces the principle that policing powers must be applied lawfully and proportionately.

Deployment decisions and actions must be guided by the National Decision Model (NDM), ensuring that officers consider the Code of Ethics at every stage. This includes applying principles of fairness, integrity, accountability, and respect when responding to alerts and engaging with the public. Officers should continually review their decisions against the NDM to ensure they remain lawful, proportionate, and ethical.

The briefing will provide clear direction on Body-Worn Video (BWV) use. All officers must activate BWV for every public interaction during the deployment. Officer should comply with the BWV policy when using their BWV and when footage has been captured.

Officers must also remain aware of unconscious bias throughout the deployment. Decisions following an LFR alert must be based on objective assessment and corroborating evidence, not assumptions or stereotypes. Supervisors will reinforce this during the briefing to ensure fairness and impartiality.

8.3 Site Setup

Upon arrival at the designated deployment area, operational teams will position LFR-equipped vans and cameras in accordance with the site plan and command guidance, aiming for optimal coverage of the recognition zone. Where unforeseen circumstances arise, teams may adjust

placements as necessary, ensuring any changes remain consistent with operational objectives and compliance requirements.

Clear and visible signage will be placed around the deployment area. The purpose of this signage is to inform individuals that Live Facial Recognition technology is in use, ensuring transparency and compliance with statutory obligations under data protection and privacy legislation.

Signage should be positioned so it is easily noticeable to anyone entering or passing through the recognition zone, taking into account environmental factors such as lighting, pedestrian flow, and accessibility. Where unforeseen circumstances prevent placement at the originally planned locations, teams should select alternative positions that maintain visibility and effectiveness.

Officers should establish the Zone of Recognition (ZoR), which is the defined area within which facial images are captured by Live Facial Recognition (LFR) technology. The ZoR is determined by the field of view of the deployed CCTV cameras on the LFR vehicle.

If ZOR adjustments are required during the deployment, this must be recorded in the deployment log, including boundaries and rationale for changes, to ensure transparency and accountability.

8.4 Technical Readiness and Per□ormance Monitoring

Before deployment begins, the LFR Officer must carry out a technical check to confirm that the system is fully operational. This process starts with powering on the LFR van and ensuring that all cameras are connected and functioning correctly. The officer should verify network connectivity between the cameras, the LFR system, and the command interface, as well as confirm that logging systems and alert monitoring tools are active and responsive.

To validate system performance without using live operational data, the officer must upload a blue test watchlist from the encrypted pen drive to the NEC NeoFace system. Once the blue watchlist is loaded, a simulated detection should be performed to confirm that alerts are generated correctly. During this test, the officer is looking for several key indicators of system reliability: the alert must appear promptly in the monitoring tool with accurate details such as the image, match score, and watchlist reference; the similarity score should align with the set threshold of 0.64; and the alert must be logged accurately in the system with the correct time, date. The officer should also check that any configured notifications are triggered as expected, that alerts can be acknowledged and cleared, and that the system remains stable throughout the process with no crashes or connectivity issues. An auditable record of the test alert must be available for compliance purposes.

Once the technical checks are complete, the officer must confirm that the threshold remains set at 0.64. Finally, the officer must record the completion of these checks in the deployment log, including the date, time, their name, confirmation that the blue watchlist test was conducted, and any issues identified along with actions taken.

During deployment, environmental conditions can significantly impact the performance of Live Facial Recognition systems. Factors such as changes in crowd density, movement patterns, adverse weather conditions like heavy rain or fog, and falling light levels may affect camera visibility and image quality. If these conditions alter substantially during the operation, the LFR

Officer must conduct an additional functionality check using the blue watchlist. This test ensures that alerts continue to display correctly and that the system remains stable under the new conditions. The outcome of the test, including the date, time, and officer name, must be recorded in the deployment log to maintain an auditable record.

8.5 Monitoring Alerts

LFR operators must continuously monitor the live camera feed and the LFR system to ensure it is functioning correctly and that alerts are promptly identified. Operators should remain vigilant for technical issues or environmental factors that could affect system performance and report any anomalies immediately.48. Each alert verified by human officer before intervention.

Every system-generated alert must be reviewed and verified by an LFR operator before any intervention occurs. This process ensures that decisions are not based solely on automated outputs and helps prevent misidentification. Verification involves carefully comparing the live image captured by the system with the watchlist image, checking for distinctive facial features, and considering contextual factors such as clothing, location, and behaviour. Once the operator is satisfied that the alert is accurate, they will notify engagement officers, who will approach the individual and carry out the necessary police checks.

All alerts, whether confirmed or dismissed, along with verified matches and any subsequent interventions, must be recorded in the deployment log. Records should include time, location, operator details, verification outcome, and rationale for any action taken. This provides an auditable trail for accountability, oversight, and post-deployment review

8.6 Public Engagement

Engagement officers must remain clearly visible and readily available within the deployment area. Their presence reassures the public, supports transparency, and ensures that any verified alerts can be acted upon promptly and professionally.

When officers engage with individuals—whether following a verified alert or speaking to members of the public passing through the Zone of Recognition (ZoR)—they clearly and confidently explain the purpose of Live Facial Recognition (LFR) and outline the safeguards in place to protect privacy. Officers explain why the person has been approached (if applicable), offer an LFR information leaflet, and direct individuals to the official Merseyside Police website or the QR code on the leaflet for more details. The leaflet provides information about the technology, its legal basis, and how individuals can access further guidance or raise concerns.

9 Post-Deployment Phase

9.1 Cancellation Report

At the conclusion of the deployment, officers complete a full cancellation report to provide a comprehensive record of the operation. This report serves as an auditable document for accountability, oversight, and continuous improvement. The report will outline the operational outcomes, including the number and nature of alerts generated, arrests made, safeguarding interventions, and any public engagements that occurred outside of alert-driven interactions. It will also detail incidents and challenges encountered during the deployment, such as environmental factors, operational disruptions, or resource constraints.

Deployment logs will also be submitted to the LFR Team and stored securely online via the dedicated LFR Microsoft Teams channel, ensuring an auditable record of operational activity and compliance with governance requirements.

9.2 Governance and Reporting

Following the conclusion or cancellation of an LFR deployment, governance requirements must be fulfilled to ensure transparency, accountability, and compliance with legal and ethical standards. The LFR team will review and, where necessary, update the Community Impact Assessment (CIA) and Equality Impact Assessment (EIA) to reflect any changes arising from the operation.

Deployment results will be published online in accordance with organisational policy, providing clear information on the purpose of the deployment, its location, dates, operational outcomes, and the safeguards applied to protect privacy and proportionality. This publication ensures public visibility and supports confidence in the use of LFR technology.

Technical performance will be assessed in detail, recording any issues related to system reliability, accuracy, or functionality. Community feedback gathered during the deployment will be summarised, reflecting public engagement, concerns raised, and any reassurance measures provided.

Based on these findings, recommendations will be formulated to inform future deployments, focusing on operational effectiveness, technical resilience, and community confidence. All learning points will be submitted to the LFR Unit for inclusion in organisational learning frameworks and to support continuous improvement across all deployments.

These outcomes and records will be discussed by the Senior Responsible Officer (Ch/Supt Thornton) and ACC Wilson, during governance meetings to ensure oversight and continuous improvement.

Version History

Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1	03/12/2025	Document creation	Ch/Supt Thornton	Sgt 7649 Hilton