LIVE FACIAL RECOGNITION

POLICY & PROCEDURE

OFFICIAL

Publication Scheme	Government Security Classification Scheme (GSCS): **OFFICIAL** Publish Policy & Procedure on External Force Website? **Yes - Policy and 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)	Authorised Professional Practice Live facial recognition | College of Policing Facing the Camera: Good practice and guidance Regulation of Investigatory Powers Act 2000 ICO Opinion: The Use of LFR in public spaces 2021 Protection of Freedoms Act 2012 R (Bridges) -v- CC South Wales _ors Judgment Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects Data protection: The Data Protection Act Review, Retention & Disposal; Records Management Policy and Procedure Review, retention and disposal APP
This Version	1.0
Date Created / Modified	02/12/2025
Date Last Approved at SMB	02/12/2025
Review By	02/12/2028

Contents

Policy

Statement

Across UK policing, biometric technologies, particularly Live Facial Recognition (LFR), are increasingly recognised as valuable tools for supporting crime prevention, safeguarding, and public protection.

LFR can assist in locating individuals where intelligence suggests they may pose a risk of harm to themselves or others. This includes those considered vulnerable such as missing persons, to locate and arrest individuals wanted for criminal offences, and to protect public spaces and events from individuals subject to legal restrictions.

Merseyside Police will deploy Live Facial Recognition to address threat harm and risk and in a manner that is intelligence-led, time-bound, and governed by rigorous safeguards to ensure its lawful, ethical and transparent use.

Each deployment will be authorised through a formal process and evaluated for accuracy, impact, and fairness. Merseyside Police will ensure that all deployments are overt, legally justified, and subject to public engagement. The force will ensure accountability through structured governance and legal compliance.

The force aligns its approach with key national frameworks to maintain consistency and accountability:

- *Authorised Professional Practice (APP),* issued by the College of Policing, provides operational guidance for officers and staff. Merseyside Police refer to APP as the primary source of professional standards and will develop local procedures only where necessary to support specific operational needs.
- The Surveillance Camera Commissioner's Code of Practice sets out principles for the responsible use of surveillance technologies. Officers follow this code to ensure transparency, proportionality, and public confidence in LFR deployments.
- Guidance from the Information Commissioner's Office (ICO) informs Merseyside Polices data protection practices. Merseyside Police engages with ICO standards to ensure that all biometric data processing complies with the Data Protection Act 2018 and UK GDPR.

Aims

This policy sets out a clear framework for the lawful, ethical, and proportionate deployment of Live Facial Recognition (LFR) technology by Merseyside Police. It enhances operational effectiveness, safeguards vulnerable individuals, and ensures robust governance and oversight. The policy supports compliance with national standards and promotes public trust in the responsible use of biometric technologies.

Objectives

This policy sets out how Merseyside Police will use Live Facial Recognition (LFR) technology. It informs staff and the public about LFR's purpose, provides officers with clear deployment guidance, outlines the governance and legal oversight framework, and explains the technology's role in operational policing.

Rationale

This policy provides a clear and accountable framework for Merseyside Police's use of Live Facial Recognition (LFR). It ensures deployments are lawful, ethical, and transparent, in line with legal duties under the Human Rights Act 1998, Data Protection Act 2018, Equality Act 2010, and consistent with national guidance. The policy is essential to safeguard individual rights while supporting public safety and operational effectiveness.

Application and Scope

This policy applies to all Merseyside Police officers, staff, volunteers, and contractors involved in LFR. The policy covers LFR used by Merseyside Police. It does not apply to facial recognition systems operated by other agencies or companies, nor to Operator-Initiated Facial Recognition (OIFR), Retrospective Facial Recognition (RFR), or covert surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA).

This policy provides guidance to officers and staff on the effective and lawful use of Live Facial Recognition (LFR). While it sets out operational standards, it is vital that officers and staff retain the discretion to make decisions based on the specific circumstances of each case. This ensures that LFR supports policing objectives without replacing professional judgement or undermining individual accountability.

Strategic oversight of LFR within Merseyside Police is provided by the Assistant Chief Constable responsible for Matrix Force Operations, who serves as the Chief Officer lead for this area. The Senior Responsible Officer is Chief Superintendent Head of Matrix & Force Operations.

Outcome Evaluation

At every stage of Live Facial Recognition (LFR) operations, from planning to review, Merseyside Police uphold the principles of Justifiable, Proportionate, Legal, Accountable, Necessary, and Ethical.

Each deployment must formally authorise based on a clearly defined policing aim, with legal thresholds and ethical considerations carefully assessed. The LFR working group leads on planning, policy development, and training, helping shape deployments that are necessary and proportionate to the identified need.

During live operations, Merseyside Police will closely monitor system accuracy and assess key outcomes, including alerts, arrests, and any resulting interventions. Internal checks will be carried out to confirm that deployments remain lawful and ethically sound in practice.

Crime patterns for the locality of a deployment will be reviewed both prior to and following the deployment. This analysis will form part of the evaluation process to assess the effectiveness and appropriateness of the deployment. The review will consider whether the deployment contributed to reducing crime or addressing the identified issues and will inform future operational decisions.

Where appropriate, independent audits will be commissioned to provide external scrutiny and support transparency. Following each deployment, the LFR working group will conduct a structured review of results to identify learning, assess proportionality, and guide future deployments.

Public engagement is a key part of our approach. Feedback will be gathered through community meetings, online platforms, and structured engagement activities. Insights and performance data will be published in annual reports, reinforcing our commitment to accountability and public trust.

Procedure

Version History

Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1	02/12/2025	Version 1 Approved by SMB 2/12/25	Ch/Supt Thornton	Sgt 7649 Hilton

1. Procedure Guidance

1.1.1 This section outlines the steps Merseyside Police will follow to ensure the lawful, ethical, and effective deployment of Live Facial Recognition (LFR) technology. Procedures are aligned with Authorised Professional Practice (APP) unless explicitly justified otherwise. Roles and responsibilities are clearly defined.

1.1.2 Merseyside Police acknowledges that LFR invokes debate about the ethical implications of its use. Merseyside Police has undertaken an extensive consultation process and reviewed the National Physical Laboratories (NPL) equitability study to ensure that LFR, when deployed in an operational context, is used in a fair, transparent and lawful way which does not unfairly disadvantage any community.

1.1.3 LFR is a targeted intelligence led policing tool. Merseyside Police does not operate LFR as a tracking tool for wide-scale monitoring of the public, or as an autonomous decision-making capability.

1.1.4 LFR can help keep the public safe by assisting Merseyside Police to identify individuals who are on a pre-determined watchlist within a zone of recognition at a pre-determined location.

1.1.5 LFR works by analysing facial features, which generates a mathematical representation. The representation is compared against known faces in a watchlist to find matches. If a match is identified, the system alerts the trained operator. The operator reviews the match and decides whether to take further action. In this way, LFR works to assist Merseyside Police officers to make decisions, rather than independently or autonomously making decisions.

1.1.6 LFR will only be used as a policing tool by Merseyside Police, where the Authorising Officer (AO) considers it necessary, proportionate, legitimate and lawful.

1.1.7 LFR will only be used as a policing tool by Merseyside Police where the AO considered the Human Rights and wider impact on individuals and communities and employs control measures to mitigate the collateral intrusion and impact.

1.1.8 Merseyside Police will continually monitor the impact of LFR, through existing and new governance processes. This governance process will test the efficacy and equality impact of LFR.

1.1.9 This LFR Policy will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

2. Use of LFR

2.1.1 This policy relates to the use of LFR in an overt capacity to aid Merseyside Police to protect the public, pursue offenders and prevent crime.

2.1.2 LFR can recognising persons from a large dataset, more effectively than individual officers at a location.

2.1.3 LFR will only be used as a policing tool by Merseyside Police, where the LFR Operators and LFR Engagement Officers are trained in their roles and the use of the LFR equipment.

2.1.4 LFR should only be deployed, unless justified otherwise, with the appropriate resources required to act on any alerts as they are generated.

2.1.5 Merseyside Police will deploy LFR using dedicated CCTV systems, including static cameras and liveried vehicles positioned in strategic locations.

2.1.6 LFR deployment locations must be kept under review and LFR should be deployed to locations that are supported by a rationale for their selection. This will be auditable and in accordance with the principles set out in the legal mandate.

2.1.7 LFR, deployments are categorised into three types:

a) Proactive Deployments

Deployments based on crime data, intelligence, and operational analysis. These are used in areas experiencing persistent or high-volume criminal activity, or where there is a known risk of harm. LFR may be deployed at access routes, transport hubs, or public spaces where its use can support crime prevention, detect wanted or vulnerable/missing persons, and in doing so provide public reassurance. Watchlists must be linked to the policing purpose for which LFR is deployed, and there must be reasonable suspicion that individuals on the watchlist may attend the location.

b) Event Deployments

Planned deployments in response to specific events expected to attract large public attendance, such as concerts, sporting fixtures, public gatherings, assemblies and celebrations. These support public safety, protect critical

infrastructure, and prevent disorder. Deployment locations may include the event site, surrounding areas, and transport routes.

c) Incident/Intelligence-Specific Deployments

Reactive deployments in response to a specific incident or credible intelligence. These may be used to locate suspects, support safeguarding interventions for vulnerable or missing person, or prevent imminent harm. Watchlists are tightly focused on the geographical area and individuals relevant to the incident or intelligence.

3. Governance, Oversight and Impact Assessments

3.1.1 Merseyside Police recognises that the benefits to the public of deploying LFR should be balanced against public confidence. The deployment authorisation process and governance arrangements are designed to continually test that balance.

3.1.2 The authority to deploy LFR is an operational one but must be approved by an Authorising Officer. In Merseyside Police the AO is an officer of Superintendent (or above) rank.

3.1.3 Where an Authorising Officer (AO) is unable to provide written authorisation immediately, and the deployment of LFR is required urgently, verbal authorisation may be granted. In such cases, the AO must record the authorisation in writing as soon as practicable using the appropriate Merseyside Police LFR authorisation form.

3.1.4 Urgent authorisation may be justified in situations including:

a) An imminent threat to life or a serious risk of harm to individuals or property.

b) A time-sensitive intelligence or investigative opportunity, where delay would compromise the potential benefit of action.

3.1.5 All urgent authorisations must still meet the legal, ethical, and operational standards set out in Merseyside Police's LFR policy and procedure.

3.1.6 Prior to deploying LFR, or as soon as practicable after authorising in urgent cases, the AO or their delegate must inform the below in writing:

a) Duty NPCC Officer

b) Office of the Police and Crime Commissioner

c) Local Policing Area Command Team

d) Local Authority for the LPA

e) Force Incident Manager

f) Legal Services

g) Community Engagement Unit

h) Press Office

4. Overview of LFR Deployment Procedure

4.1.1 Deployment Planning and Authorisation. A clear lawful purpose must be identified. Safeguards are considered, and a senior officer authorises the deployment. A watchlist is compiled using strict inclusion criteria aligned with legal standards.

4.1.2 Pre-Deployment Notification. Public notification is issued, and clear signage is displayed at the deployment location to ensure transparency and public awareness.

4.1.3 Operational Deployment. As individuals pass the LFR camera, the system detects faces and compares them against the watchlist, provided image quality is sufficient.

4.1.4 Alert Generation and Review. If a possible match is identified, the system generates an alert. The LFR Operator or Engagement Officer reviews the alert, comparing the live image with the watchlist entry and assessing environmental and system factors.

4.1.5 Decision and Engagement. Based on training, experience, and the quality of the match, the officer determines whether further action is required and whether to engage the individual.

4.1.6 Post-Deployment Review. The deployment authority is formally cancelled, and a post-operational evaluation is conducted. This includes assessing system performance, engagement outcomes, and community impact.

5. Pre Deployment

5.1 Assessments

5.1.1 The Authorising Officer (AO) must ensure the completion and review of the following assessments prior to any LFR deployment:

a) Community Impact Assessment (CIA)

b) Equality Impact Assessment (EIA)

c) Data Protection Impact Assessment (DPIA)

d) Surveillance Camera Commissioner’s Self-Assessment code

5.1.2 Documents such as the DPIA and EIA may apply across multiple deployments. These must be reviewed regularly for sufficiency but do not require revision for each individual deployment unless circumstances change.

5.2 Operational Risk Assessment

5.2.1 A documented assessment of operational risks specific to the proposed deployment must be completed.

5.2.2 The assessment must include mitigation measures to address identified risks and ensure the safety of officers, staff and the public.

5.3 LFR Application

5.3.1 The LFR application must outline the proposed deployment and include:

a) Legitimate policing aim
b) Location
c) Dates and times
d) Legal basis
e) Necessity and proportionality
f) Safeguards
g) Watchlist composition and rationale for inclusion
h) Resources appointed

5.3.2 The application must include a summary of the intelligence case that supports the deployment, including the nature of the threat, relevant individuals, and any recent incidents or patterns that justify the use of LFR.

5.3.3 The Force Intelligence Bureau (FIB) will support the applicant by providing an intelligence case to inform the deployment.

5.3.4 Corporate Support and Development (CSD) will assist the applicant by supplying data on crime patterns and trends relevant to the proposed deployment.

5.3.5 The applicant is to use the intelligence and crime data to identify the most appropriate deployment location and determine which individuals should be included on the watch list. This assessment must include consideration of crime patterns and intelligence for the locality both prior to deployment and following deployment. Dates and times of the proposed deployment must be factored into the analysis to ensure that the timing aligns with identified crime trends and patterns.

5.3.6 The deployment location must be supported by reasonable grounds to suspect that one or more individuals on the watchlist will be present at the specified time(s). This rationale must be recorded in a manner that is clear and understandable to an objective third party.

5.3.7 The application must identify the legitimate policing aim and explain how it justifies any potential interference with rights under the European Convention on Human Rights (ECHR), including privacy, freedom of expression, and assembly.

5.3.8 The application must assess the sensitivity of the proposed location, including whether it is a place where individuals may reasonably expect a higher degree of privacy (e.g. schools, hospitals, places of worship). Additional safeguards must be considered where appropriate.

5.3.9 The application must detail the approach to:

a) Signage placement and visibility
b) Fair processing information in public spaces and online
c) How individuals can exercise their data protection rights
d) Arrangements for retention and/or disposal of personal data
e) Public messaging
f) Liaison with local stakeholders

5.4 LFR Deployment Authorisation

5.4.1 Each deployment of Live Facial Recognition (LFR) technology must be formally authorised to ensure legal compliance, operational integrity, and accountability. This authorisation must confirm that the deployment is intelligence-led, necessary, and proportionate to the policing purpose.

5.4.2 Authorisation must be granted by a Superintendent.

5.4.3 In determining whether to authorise a Live Facial Recognition Deployment, the Authorising Officer must undertake a structured three-stage assessment:

a) Firstly, the Authorising Officer must evaluate whether the deployment is necessary to achieve a legitimate policing objective, such as preventing serious crime, protecting public safety, or locating individuals of interest.
b) Secondly, Authorising Officer must identify any interference the deployment may cause to the rights and freedoms of members of the public. This includes consideration of rights protected under the European Convention on Human Rights, such as the right to privacy, freedom of expression, and other relevant legal protections.

c) Thirdly, the Authorising Officer must determine whether the level of interference identified is justified and proportionate in the specific operational context. This decision must consider the nature of the location, the scale of the deployment, and the expected impact on the public.

5.4.4 Potential Impact on Public Confidence and Participation. When considering whether to authorise a Live Facial Recognition (LFR) deployment, the Authorising Officer must assess the reasonable expectations of privacy associated with the proposed location. This assessment is a key component of determining whether the deployment is proportionate and justified in the context of Merseyside Police's operational objectives. Examples of location include hospitals, schools, polling stations, and places of worship. The timing and context of the deployment also influences privacy expectations; for instance, a venue may warrant more privacy when operating privately than during a public event. An assessment will consider whether the deployment may deter individuals from exercising their rights (e.g. attending a protest or religious service).

5.4.5 The AO must provide written authorisation confirming:

a) Accountability, legality, necessity, and proportionality

b) Adequate safeguards are in place

c) Alternatives were considered and found insufficient

5.4.6 The AO must agree the date, time, location, and duration of the deployment in advance, based on the principles of necessity and proportionality.

5.4.7 The decision must be documented in a Written Authority Document (WAD), which serves as the formal record of approval.

5.4.8 The written authorisation must be retained, and it must be available for independent inspection and review as required.

5.4.9 Where an Authorising Officer is unable to provide written authorisation immediately, and the deployment is required urgently, verbal authorisation may be granted. This must be recorded in writing as soon as practicable. Urgent authorisation may be justified in cases involving an imminent threat to life, serious harm, or time-sensitive intelligence opportunities.

5.5 Data Protection and Impact Assessments

5.5.1 Each deployment of Live Facial Recognition (LFR) technology must be supported by a Data Protection Impact Assessment (DPIA) and a Record of Processing Activity (ROPA).

5.5.2 The DPIA must outline the legal basis for processing under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), specifically referencing Part 2 for general and safeguarding related purposes and Part 3 of the DPA 2018 which governs processing for law enforcement purposes. It must also assess potential risks to individuals' rights and freedoms and detail the mitigation measures in place to address those risks.

5.5.3 The ROPA provides a structured record of how biometric data will be collected, stored, accessed, and deleted, in accordance with the principles of data minimisation, purpose limitation, and storage limitation.

5.5.4 The Data Protection Officer (DPO) is responsible for reviewing and approving the DPIA. This ensures that all processing activities are compliant with statutory obligations and internal governance standards. The DPIA and ROPA form part of the deployment audit trail and are subject to periodic review to ensure continued compliance. (See 5.1.2)

5.6 Watchlist Inclusion Criteria: Compilation and Validation

5.6.1 Watchlists used in Live Facial Recognition (LFR) deployments must be compiled lawfully and in a manner that is necessary, proportionate, and operationally justified.

5.6.2 Each watchlist must be specific to the deployment and support a legitimate policing purpose, such as locating individuals wanted for serious offences, safeguarding vulnerable persons, or preventing crime and disorder and there is a clear operational need. The following categories of individual may be considered but are not exhaustive:

a) Persons wanted for serious or recordable offences.

b) Individuals subject to court-imposed orders or banning notices, including those restricting presence in specific areas.

c) Persons linked to terrorism, including those convicted or cautioned under relevant legislation.

d) Missing persons or vulnerable individuals at risk of harm.

e) Individuals managed under Multi-Agency Public Protection Arrangements (MAPPA), where risk assessments support proactive identification.

5.6.3 All entries must be supported by current intelligence or legal status, sourced from lawfully held databases such as custody images.

5.6.4 When selecting suspects for inclusion on a watchlist, the AO should consider restricting the composition to individuals suspected of being in the vicinity of a deployment area. This means there is some possibility or likelihood that the individual will pass through the LFR deployment. The degree of likelihood required for inclusion varies between cases and should be assessed against several relevant factors.

5.6.5 An AO may deem it necessary and proportionate to authorise the inclusion of people on a watchlist, even though there may not be specific intelligence to say where they might be found. 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) 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. For example, areas around transport hubs have a lot of people transiting from place to place.

5.6.6 The compilation of watchlists must comply with the Data Protection Act 2018 and UK GDPR, particularly in relation to the lawful processing of biometric data for law enforcement purposes. The principles of necessity, proportionality, and data minimisation must be applied throughout.

5.6.7 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.

5.6.8 Watchlists must be reviewed prior to each deployment. Entries must be removed when no longer justified to ensure the use of biometric data remains targeted, proportionate, and aligned with legal and ethical standards.

5.7 Public Notification

5.7.1 Merseyside Police will provide advance public notification of Live Facial Recognition (LFR) deployments. Notification will be issued via the force website and media channels at least five days prior to deployment.

5.7.2 A structured public communication strategy will support LFR deployments, including the force website, social media updates, FAQs, and community briefings.

5.7.3 Merseyside Police will create a dedicated Live Facial Recognition (LFR) webpage to support transparency and public engagement. The page will explain how LFR works, provide details of upcoming and past deployments, outline how biometric data is processed and deleted, describe the criteria for inclusion on watchlists, and offer contact information for public enquiries and feedback.

5.7.4 Merseyside Police recognise the public's right to access personal data under UK GDPR and the Data Protection Act 2018. Individuals may submit Subject Access Requests (SARs) to understand whether and how their data has been processed during LFR deployments. Guidance on how to make a SAR will be made publicly available via the Merseyside Police LFR webpage and will also be provided through signage and leaflets at deployment locations to support transparency and accessibility.

6. Deployment Phase

6.1.1 To ensure lawful, proportionate, and transparent use of Live Facial Recognition (LFR) technology, the following procedures must be followed on the day of deployment:

6.1.2 LFR officers are to generate the watch list on the day of deployment to ensure its currency and accuracy. The watch lists will be compiled using the nationally approved templates provided by the National LFR Team, ensuring consistency with other forces. Categories for inclusion may include, but are not limited to:

a) Terrorism-related subjects
b) Individuals wanted on warrant
c) Registered Sex Offenders (RSOs)
d) Persons wanted for crimes circulated on PNC
e) Subjects with Criminal Behaviour Orders (CBOs)
f) Missing persons (MISPERs)
g) Event-specific persons of interest
h) Individuals subject to recall to prison
i) Other categories as defined by the Authorising Officer (AO)
j) Police test lists

6.1.3 There will be a structured briefing for all officers and staff involved in the deployment, including LFR operators, engagement officers and supervisory or command roles. The pre-deployment briefing outlines the operation's objectives and the watchlist in use. The briefing also covers legal powers, ethical considerations, public engagement plans, and data protection responsibilities.

6.1.4 Officers are assigned roles and given clear instructions on responding to alerts and non-alerts.

6.1.5 Prior to LFR activation, officers are to carry out a full check of the LFR system to ensure it is fully operational and correctly configured. They will confirm that all cameras are positioned as planned and functioning correctly, with clear coverage of the designated

area, and that the system's connectivity and data storage functions are tested to ensure secure and uninterrupted operation throughout the deployment.

6.1.6 Officers are to ensure the software is calibrated to the appropriate threshold settings to balance recognition accuracy with the need to minimise false alerts.

6.1.7 Officers will ensure that signage is clearly displayed at all entry points to the Zone of Recognition to inform the public of the LFR deployment.

6.1.8 Uniformed officers and engagement staff will be deployed to provide information inclusive of leaflets and respond to public queries.

6.1.9 During deployment, officers will monitor system-generated alerts in real time. All potential matches must be subject to human adjudication before any action is taken.

6.1.10 Officers will ensure that any member of the public engaged due to an alert is informed of the reason and provided with further information if requested.

6.1.11 If no engagement officer is available to assess and act on alerts, the LFR system must not be used. The system is paused or stood down until engagement capability is restored.

6.1.12 Operational logs must be maintained throughout the deployment. These logs will record key decisions, alerts reviewed, officer responses, and outcomes such as the number of alerts, number of engagements, number of arrests and safeguarding interventions.

6.1.13 This documentation forms part of the deployment audit trail and supports post-deployment evaluation, governance review, and external scrutiny.

6.1.14 All biometric data that does not result in watchlist alert, is automatically deleted by the LFR system during deployment. The LFR system is designed to process facial images in real time and immediately discard non-matching biometric data, ensuring compliance with data protection legislation and minimising unnecessary retention.

6.1.15 At the conclusion of every deployment, LFR officers must generate a system report. This report will include all confirmed matches against the operational watch list, any matches against the Blue Watchlist (used for system testing and assurance), the total number of faces scanned, and the operational times (start and end). This ensures transparency, supports post-deployment evaluation, and demonstrates system integrity

6.1.16 The report must be retained in accordance with force policy, data protection legislation, and the Police Information and Records Management Code of Practice (MoPI).

6.1.17 It is the responsibility of LFR Supervisor to ensure that all watch list data is wiped immediately following the conclusion of the deployment, or as soon as practicable. This includes any locally stored copies and system data, in compliance with data protection requirements and force policy.

7. Post-Deployment Review and Reporting

7.1.1 A cancellation report must be completed by an LFR supervisor and reviewed by the Authorising Officer. This report will document the deployment's outcomes, including the number and nature of alerts, enforcement actions taken, and any safeguarding interventions. It will also assess the deployment's alignment with the original operational rationale and legal authorisation.

7.1.2 The cancellation report must be sent to the following in writing by the AO or an LFR delegate,

a) Duty NPCC Officer
b) Office of Police and Crime Commissioner
c) Local Policing Area Command Team
d) Local Authority for the LPA
e) Force Incident Manager
f) Legal Services
g) Community Engagement Unit
h) Press Office

7.1.3 Following each deployment of Live Facial Recognition (LFR) technology, Merseyside Police will conduct a structured post-operational review.

7.1.4 To support compliance and operational integrity, automated deletion protocols will be applied wherever possible, ensuring that data is not held longer than necessary and that all processing remains lawful, proportionate, and accountable.

7.1.5 Following each deployment, a performance summary will be published online to ensure transparency and accountability. The report will include the following metrics:

a) Deployment Location
b) Date
c) Start & Finish Time
d) Watchlist Size
e) Total Alerts

f) True Alerts Confirmed

g) True Alerts Unconfirmed

h) False Alerts Confirmed

i) False Alerts Unconfirmed

j) False Alert Rate

k) Outcome – Arrest

l) Outcome – Other

m) No Action

n) Faces Seen

These metrics will be compiled from system data and operational logs by the LFR team, reviewed internally for governance, and published on the force's website.

7.1.6 Wider performance metrics such as community feedback, public sentiment, complaints, and engagement outcomes will also be used to inform future deployments and support ethical decision-making.

7.1.7 Lessons learned will be documented and shared with all governance and oversight structures, including community scrutiny meetings such as the Merseyside Independent Advisory Group, Police Race Action Plan Stakeholder Group and Police and Crime Commissioner Scrutiny meetings, to support organisational learning and demonstrating that we are publicly accountable.

8. Training and Awareness

8.1.1 Merseyside Police will implement a structured training programme for all personnel involved in LFR operations. This training will cover:

a) Legal Compliance: Understanding relevant legislation, including data protection and human rights obligations.

b) Bias Mitigation: Techniques and awareness to reduce discriminatory outcomes and ensure fair use.

c) Public Engagement: Best practices for interacting with the public during deployments, including transparency and accountability.

8.1.2 Training procedures are aligned with Authorised Professional Practice (APP) unless explicitly justified otherwise. Training records will be maintained and oversight of training records we be continuously monitored.

8.1.3 Roles and responsibilities will be clearly defined, and technical content will be structured to support operational clarity and ease of navigation.

9. Addressing Disproportionality, Bias and Over-Policing of communities

9.1.1 Merseyside Police recognise the historic over-policing of minority communities and the impact on their confidence in policing. We acknowledge that Live Facial Recognition (LFR) may raise concerns among all communities, particularly visible minority groups. This policy commits to addressing these concerns through transparency, accountability, and proactive engagement.

9.1.2 Merseyside Police has undertaken an Equality Impact Assessment for its use of Live Facial Recognition (LFR).

9.1.3 Merseyside Police does not create or retain a breakdown of race, gender or any other protected characteristic of persons on a watchlist.

9.1.4 The Deployment of LFR is driven by Merseyside Police 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.

9.1.5 Merseyside Police recognise 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, in accordance with its obligations under equality and date protection legislation.

9.1.6 Any use of LFR technology through mutual aid, will only be allowed where the providing force has bias safeguards in place. Merseyside Police is aware that forces providing LFR on mutual aid have several 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 LRF Supervisor will halt the deployment where necessary; and

b) To 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; and

c) If post-deployment reviews identify an area of concern, further equitability testing will take place where this appears necessary.

9.1.7 Post-deployment reviews will include opportunities for independent scrutiny. Where appropriate, members of advisory groups such as the Merseyside Independent Advisory Group (MIAG) will be invited to participate.

10. Mutual Aid

10.1.1 At this time Merseyside Police does not operate its own LFR physical assets or operating platform and will only operate LFR through mutual aid. Merseyside Police will only operate LFR where the authorising officer is satisfied that the equitability has been proven.

10.1.2 Mutual Aid can be supplied by the Metropolitan Police, South Wales Police or Greater Manchester Police. These forces operate LFR on the NEC operating platform.

10.1.3 Merseyside Police is aware that forces providing LFR on mutual aid have several 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.

10.1.4 Merseyside Police will complete system checks to address any potential bias, as detailed in the 'deployment' section of this document.

10.1.5 The Northwest regional LFR asset, held by Greater Manchester Police (GMP), operates using the NEC NeoFace system. This system has been assessed by the National Physical Laboratory (NPL) and validated by National Institute of Standards and Technology (NIST) as one of the most accurate and equitable facial recognition technologies available. NPL testing confirmed that at a face-match threshold setting of 0.64, the system achieves high accuracy and shows no statistically significant bias across demographic groups. This threshold exceeds the recommended minimum of 0.6 and reflects best practice for reducing false positives and ensuring fairness.

10.1.6 Where other systems are used under mutual aid arrangements Merseyside Police will require similar evidence of independent testing and bias mitigation measures to maintain transparency and public confidence in the use of LFR technology.

11. Oversight and Data Protection

11.1.1 The Merseyside Police Senior Responsible Officer for LFR is Chief Superintendent Matrix Force Operations.

11.1.2 The SRO will liaise as necessary with National Police Chief Council (NPCC) ranked officers and Merseyside's Police and Crime Commissioner. The SRO chairs the Facial Recognition Technology Board which will review the

11.1.3 The SRO will retain responsibility for policy and procedure relating to LFR and will engage and support all levels of the Command structure in the review of LFR usage and outcomes.

11.1.4 The senior oversight board for LFR is the Strategic Public Order Public Safety meeting chaired by ACC Matrix and Response and Resolution.

11.1.5 LFR will be governed through the Strategic Public Order Public Safety meeting, reporting into Strategic Management Board. Thematic reviews will be commissioned every six months through Public Encounter Group and Merseyside Independent Advisory Group.

11.1.6 The Merseyside Office of the Police and Crime Commissioner can also provide an independent oversight function via the quarterly PCC Scrutiny Boards (Note Draft APCC LFR MOU).

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

11.1.8 Further oversight opportunities may arise from the Information Commissioners Office, the Surveillance Camera Commissioner, and the Biometric Commissioner.

11.1.9 Surveillance Camera Commissioner (SCC); The role of the Surveillance Camera Commissioner is to encourage compliance with the surveillance camera code of practice, review how the code is working, and provide advice to ministers on whether the code required amendment. Any use of a LFR system by Merseyside Police will need to comply with this code and the twelve guiding principles. This guidance document seeks to apply those principles.

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

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

11.1.12 A Data Protection Impact Assessment (DPIA) has been undertaken in relation to Merseyside Police's use of LFR. The Data Protection Impact Assessment must comply with sections 35 – 40, (Principles 1–6) and s64 Data Protection Act and should be shared with the ICO.

12. General Data Protection Regulation Assessment

12.1.1 A Data Protection Impact Assessment has been undertaken in relation to Merseyside Police's use of LFR.

12.1.2 When relying on the Schedule 1 conditions of the DPA 2018, for processing special category data. Merseyside Police must have an appropriate policy document in place. This document sets out how the organisation ensures compliance with the principles in Article 5 of the UK GDPR, such as the retention and erasure of such personal data.

12.1.3 This section explains the processing and satisfies the requirements of Schedule 1, Part 4 of the DPA (APD and Additional Safeguards).

12.1.4 Description of Data Processed - The special category data processed utilising LFR: -

a) Biometric data for the purpose of uniquely identifying a natural person.

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

12.1.6 The watchlist for LFR is primarily a subset of the Merseyside Police custody image dataset but may also include other lawfully held images. All images must be to the right standard to enable effective identification.

12.1.7 All watchlist images will have a biometric template created (special category data) at the point of enrolment to the FRT application.

12.1.8 All faces compared against the Watchlist have a biometric template created, which is considered special category personal data.

12.1.9 Biometric data used to uniquely identify an individual is special category data. For this processing we will be collecting the personal data of members of the public which will include an image that may be utilised by extracting a biometric template from it for the purposes of uniquely identifying them. Where this data does not generate an alert against that held on the watchlist it will not be further processed and biometric data of the natural person permanently deleted once this comparison has been completed. No other personal identifiers are collected in addition to the biometric image.

12.1.10 Merseyside Police maintain a record of its processing activities in accordance with Article 30 of the UK GDPR.

12.1.11 GDPR conditions for processing special category data

a) Merseyside Police processes special categories of personal data under the following GDPR Articles (lawful conditions for processing special categories of personal data under GDPR): Article 9(2)(g) - Substantial Public Interest e.g. Identification of missing persons or safeguarding children or vulnerable individuals.

b) Section 10 DPA supplements Article 9 GDPR, requiring the following conditions of Schedule 1 to be satisfied where Merseyside Police rely on Article 9(2)(g).

12.2 Schedule 1 Data Protection Act 2018 Condition for processing

12.2.1 Merseyside Police process special criteria data for the following purposes identified in paragraphs 6 and 18 of Part 2 of Schedule 1 (substantial public interest conditions):

12.2.2 Paragraph 6 – Statutory and government purposes - exercise of function conferred upon a person by enactment or rule of law:

a) This condition is met if the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and for reasons of substantial public interest.

b) The police have a common law duty not only to prevent and detect crime but to protect the public and preserve life and property: this is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions. The processing is also necessary for reasons of substantial public interest, that is, the safety and protection of the public. In determining necessity, Merseyside Police will always consider whether less intrusive measures can be used without compromising the objective and the interests of the individual balanced against the interests of the community.

12.2.3 Paragraph 18 - Safeguarding of children or individuals at risk

a) This condition is met if the processing is necessary for the purposes of protecting an individual under 18 (or over 18 and at risk i.e. vulnerable for reasons defined in the paragraph 18) from neglect or physical or emotional harm or protecting the physical, mental or emotional well-being of an individual, where the consent cannot reasonably be given or obtained in the relevant circumstances, and the processing is necessary for reasons of substantial public interest.

12.3 Procedures for ensuring compliance with the principles in Article 5 GDPR

12.3.1 Accountability Principle (Article 5(2) GDPR). Merseyside Police have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

a) The appointment of a Data Protection Officer who is responsible for data protection in relation to LFR and who reports directly to the Chief Officer team for Merseyside Police.

b) Taking a 'data protection by design and default' approach to our activities.

c) Maintaining documentation of our processing activities - (ROPA).

d) Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.

e) Implementing appropriate security measures in relation to the personal data we process.

f) Carrying out Data Protection Impact Assessments (DPIA) for our high-risk processing.

g) Merseyside Police regularly review our accountability measures and updated or amend them when required. This is auditable.

12.4 Principle (a): lawfulness, fairness and transparency

12.4.1 Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

12.4.2 We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, and this policy document. The DPIA for LFR gives specific detail regarding the way in which data is processed and how the measures we have in place ensure that the processing is lawful, fair and transparent.

12.4.3 The processing of data by LFR for the purposes of substantial public interest is necessary on the basis of Merseyside Police common law functions which might fall outside strict law enforcement purposes (for which data would be processed under Part 3 DPA); and it is proportionate to the aims pursued (see above conditions for processing where the legislative conditions on which Merseyside Police relies are explained and examples of purposes that meet each of those conditions). Merseyside Police practices respect the right to data protection and employ suitable and specific measures to safeguard the fundamental rights and interests of the data subject in so far as is necessary and lawful in a democratic society. Merseyside Police will always consider whether the use of LFR is strictly necessary (i.e. considering other measures not involving the processing of special category data and whether they could achieve the same outcome) and will ensure that at least one relevant GDPR condition or processing of specific category data and attendant DPA requirements are satisfied.

12.5 Principle (b): purpose limitation

12.5.1 Merseyside Police processes personal data where it is necessary for the purposes of protecting the public, fulfilling the common law functions to preserve and protect life and property, and to safeguard children and vulnerable persons, all in the substantial public interest as explained above.

12.5.2 This data will not be further processed for purposes which are incompatible with the purpose for which it was collected.

12.5.3 We will only share this personal data with another organisation where there is a legal power to do so and in accordance with data protection requirements.

12.5.4 This means that Merseyside Police consider what it seeks to achieve, whether there are alternative measures which would not involve processing special criteria data, but which would achieve substantially the same outcomes, and the same or lesser impact on individuals and the community.

12.5.5 If Merseyside Police is sharing collected data for one of its lawful purposes with another controller, it will document that they are authorised by law to process the data for a lawful purpose under data protection legislation and that the processing is necessary and proportionate to that purpose.

12.5.6 Merseyside Police will not process personal data for purposes incompatible with the original purpose for which it was collected.

12.5.7 Merseyside Police will not process data collected for a law enforcement purpose (for which, see the APD for Part 3 DPA) for a purpose that is not a law enforcement purpose unless the processing is authorised by law and meets the requirements of the GDPR and DPA.

12.6 Principle (c): data minimisation

12.6.1 Merseyside Police processes personal data necessary for the specified purposes and ensures it is adequate, relevant and not excessive in relation to the purpose(s) for which it is processed. The information it processes is only that which is necessary for and proportionate to its purposes. Where personal data is provided to Merseyside Police or obtained by it, but is not relevant to its stated purposes, it will be erased. An example would be if another individual's image was captured that was not subject to an enquiry.

12.6.2 In addition, Merseyside Police require the data to be of an acceptable quality for comparison e.g. an image of a face with a minimum of fifty pixels between the eyes of the subject. For LFR, this is sufficient facial biometric data to compare against a Watchlist.

12.6.3 Ultimately an LFR Operator will determine whether a match is made between the probe and candidate image after an alert. This is an additional safeguard against identification of similar but incorrect individuals.

12.7 Principle (d): accuracy

12.7.1 Merseyside Police will retain the probe image of the individual and biometric template for no longer than is necessary for non-law enforcement purposes for which it is processed. The source system (Niche RMS) image will be maintained in accordance with the Management of Police Information (MOPI). The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated). For images where an alert is generated the probe image and biometric template will be deleted as soon as practicable and within 24 hours. The comparison process takes a matter of seconds. After an Alert is generated, an LFR Operator will review.

12.7.2 Where Merseyside Police become aware that personal data contained within a watchlist is inaccurate or out of date, having regard to the purpose for which it is being processed, Merseyside Police will take every reasonable step to ensure that data is erased or rectified without delay. If a decision is made not to either erase or rectify it, for example because the lawful basis relied on to process the data means these rights don't apply, Merseyside Police will document the decision and take appropriate steps to inform the data subject. Where it is erased or rectified Merseyside Police will inform any recipients with whom it has shared that data.

12.7.3 The performance of LFR will be reviewed for accuracy.

12.8 Principle (e): storage limitation

12.8.1 The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated). For images where an alert is generated the probe image and biometric template will be deleted as soon as practicable and within 24 hours. Merseyside Police determine the retention period for this data based on its legal obligations and the necessity of its retention for business needs. The retention schedule is reviewed regularly and updated when necessary.

12.8.2 In limited circumstances images and biometric templates will be used for research purposes and evaluation of the effectiveness and performance of FRT. Where possible personal data will be anonymised or pseudonymised. Personal data being processed for research purposes will be done so in accordance with data sharing agreements requiring sufficient guarantees around the security of the information in transit and at rest, including physical, personnel and technical security measures. Such measures will be subject to scrutiny by Force Information Security Officers and the Data Protection Officer.

12.9 Principle (f): integrity and confidentiality (security)

12.9.1 Personal data processed by LFR is processed within the accredited secure computer network which is located locally within the host force area, in accordance with national and local security policies. Hard copy information is processed in line with information management policies. Data Protection Polices are applied from inception of initiatives to ensure legislative compliance with the data protection obligations and to determine appropriate levels of technical and organisational safeguards and controls when processing personal data and sensitive data. All the security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

12.9.2 The electronic systems and physical storage have appropriate access controls applied including for example, multi-factor authentication to access mobile devices (in the form of multiple signs in/access codes/facial recognition etc), password protection, encryption and locking mechanisms. Information Asset Owners are responsible for ensuring that all information management processes are applied to information and there is a continuous cycle of review and information risk identification and management. LFR has also been subject to a robust DPIA.

12.9.3 All staff receive basic data protection training and must undertake annual mandatory training for managing information. Specific training is provided to officers working with LFR which is supplemented with bespoke Standard Operating Procedures.

12.9.4 The systems in use to process personal data allow Merseyside Police and the force supplying mutual aid to respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information regarding data subjects is held. All events which take place on operation systems are recorded on an audit log which enables identification of the action executed, when it was carried out and by whom.

13. Retention and Erasure of Data

13.1.1 LFR Applications and Authorisation logs are retained in line with the NPCC retention schedule and the force Review Retention and Disposal policy.

13.1.2 Where the LFR deployment does not generate an Alert, then a person's Biometric Template and Probe Image are immediately automatically deleted.

13.1.3 Where the LFR system generates an Alert all personal data (to include Biometric Template and Probe Image) is deleted as soon as practicable and in any case within 24 hours following the conclusion of the deployment.

13.1.4 The data held on the encrypted USB memory stick used to import a watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.

13.1.5 Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.

13.1.6 LFR Operator and Engagement logs are retained in line with the NPCC retention schedule and the force Review Retention and Disposal policy.

13.1.7 All CCTV footage generated from LFR Deployments is deleted within 31 days, except were retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996.

Appendices

Appendix 1 – LFR Terminology

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

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

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

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

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

True Recognition Rate
It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated).
This is also referred to as the true positive identification rate.

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

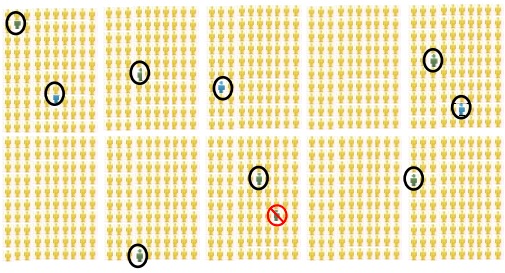
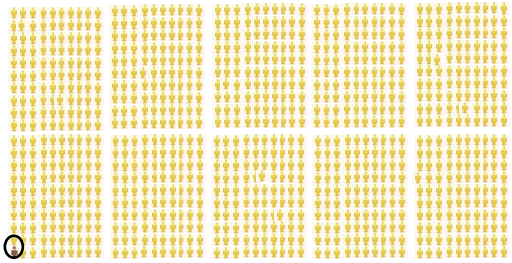
Confirmed False Alert
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

False Alert Rate

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

Application Accuracy

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

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

Authorising Officer (AO)
The officer (usually holds the rank of Superintendent or above) who provides the authority for LFR to be used.

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

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

Candidate Image
Image of a person from the watchlist returned because of an alert.

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

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

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

Engagement
An officer communicating with a member of the public because of an alert.

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

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

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

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

Gold (Strategic) Commander
Is the officer who assumes overall command, which within Merseyside Police would be the Strategic POPS Commander for a specific operation, or the duty NPCC officer. They are ultimately accountable for policing tactics for an operation or the force area.

Live Facial Recognition (LFR)
LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist 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 Merseyside Police deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of Merseyside Police LFR system.

Person(s) of Interest
A person on a watchlist.

Possible Match
A person returned because of the probe and candidate image being of sufficient similarity above the threshold.

Probe Image
A facial image which is searched against a watchlist.

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

Retrospective Facial Recognition (RFR)
A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database to identify them.

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

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

Special Category Data
Is a type of personal information that require extra protection due to its sensitive nature. In context of LFR this includes biometric data for unique identification.

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

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

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

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

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

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