Appropriate Policy Document: Live Facial Recognition Compliance with Part 3 of the Data Protection Act 2018 – Law Enforcement Processing

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.* **Publish on External Force Website? -** Yes
Department of Origin	*Matrix Force Operations*
Policy Holder	*Chief Supt Zoe Thornton*
Policy Author	*Sgt Chris Hilton*
Data Protection Officer	Ian Boyham
This Version	1
Date Created / Modified	06/12/2025
Review By *(3 years)*	

Objective

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

This document is a policy for special category data and/or criminal offence data processing by the force as part of Live Facial Recognition ("LFR"). Where there are potentially high risks because of specific processing activities, a tailored policy document will be produced in respect of that activity, however this will be on an exceptional basis.

Compliance with Part 3 of the Data Protection Act 2018 – Law Enforcement Processing

For LFR we only process biometric (facial) and limited criminal offence data necessary for policing. We do not process other sensitive categories (e.g., politics, religion, sexual orientation).

Special Category Data	Indicator X	Description of Data
Data revealing race or ethnic origin	☐	
Data revealing political opinions	☐	
Data revealing religious or philosophical beliefs	☐	
Data revealing trade union membership	☐	
Genetic data	☐	
Biometric data (used for identification purposes)	☒	Live Facial Recognition is a deployment of Facial Recognition Technology which compares a biometric template extracted from a still image of an individual immediately captured on a live feed camera and compared against an image reference database in order to assist an officer identify the subject.
Data concerning a person's sex life	☐	
Data concerning a person's sexual orientation	☐	

Criminal Offence Data	Indicator X	Description of Data
Criminal Activity	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Allegations (including unproven allegations)	☐	
Criminal Investigations	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Proceedings	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Offences	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Penalties/Sanctions/Fines	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody

Information about the absence of convictions	☐	
Conditions or restrictions laced on an individual as part of the criminal justice process	☒	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Civil Measures which may lead to a criminal penalty if not adhered to.	☐	

2. Schedule 2 DPA 2018 Condition for Processing

These legal conditions allow us to process biometric and criminal offence data for reasons of public interest, such as preventing crime, protecting the public, and safeguarding vulnerable people.

Schedule Conditions Indicator Sensitive processing of biometric data for law enforcement purposes is carried out under the conditions set out in **Schedule 1 of the Data Protection Act 2018**.	Indicator "x"	Description of Data
Administration of justice	☒	Data processed to support criminal investigations, prosecutions, and court proceedings.
Protecting vital interests	☒	Data processed where necessary to protect someone's life or prevent serious harm.
Safeguarding children and individuals at risk	☒	Data processed to locate missing persons or protect vulnerable individuals from harm.
Preventing threats to public security	☒	Data processed to prevent or respond to terrorism, serious violence, or other threats to public safety.

3. Ensuring Compliance with the Principles

Merseyside Police ensures compliance with the Data Protection Principles as set out in the Data Protection Act 2018. Full details are recorded in supporting documentation, including:

- **Privacy Notice**:
- **Data Protection Impact Assessment (DPIA)**:
- **Policies and Procedures**:

There is no requirement to reproduce information which is recorded elsewhere. Where appropriate, this APD references existing documentation to demonstrate compliance.

In addition, we record the following information to ensure compliance,

- **Deployment Application / Authorisation /Cancellation Report**
- **Deployment Log**
- **Operational Order**

These documents detail, compliance with authorisation, outcomes, and lessons learned. The report will be retained for audit and governance purposes and reviewed as part of our continuous improvement process.

Principle (a) Lawfulness, fairness and transparency We must use Live Facial Recognition (LFR) legally, fairly, and openly. This means having a clear legal basis, treating people fairly, and making sure the public knows when LFR is in use.	
Question	Details
Have we identified a lawful basis and conditions for processing sensitive data?	Lawful Basis and Conditions Lawful Basis: Section 35(2) DPA 2018 – Processing is necessary for law enforcement purposes. Special Category Data Condition: Schedule 1, Part 2 – Substantial Public Interest (Paragraphs 10, 11, 14, 18). Criminal Offence Data Condition: Schedule 1, Part 3 – Statutory and Government Purposes (Paragraph 36) and Administration of Justice (Paragraph 37). In simple terms, these legal conditions allow us to process biometric and criminal offence data to prevent crime, protect the public, and safeguard vulnerable people
Do we provide clear privacy information to the public?	Merseyside Police makes appropriate privacy information available regarding the processing of special category and criminal offence data for Live Facial Recognition (LFR). This includes: • **Privacy Notice** published on the Merseyside Police website • **Signage** at ingress and egress points of each location covered by LFR cameras • **Public communications** via website, social media, and media outlets prior to deployments • **Stakeholder briefings** and community engagement sessions • **Reference to Data Protection Impact Assessment (DPIA)**: These measures ensure compliance with the transparency principle and allow individuals to understand how their data is processed.
Are we open and honest about how LFR works?	Yes. Merseyside Police never mislead the public. We clearly explain: • Why LFR is being used. • What data is processed. • The safeguards in place. How individuals' rights are protected. Information is shared through signage, online notices, and engagement sessions.

Principle (b): purpose limitation

Personal data collected through LFR must only be used for the reason it was gathered—law enforcement. It cannot be used for anything else.	
Question	Details
Do we restrict LFR to law enforcement purposes?	Yes. LFR is only used to identify individuals on a lawful watchlist for policing purposes, such as locating wanted or missing persons.
Have we included appropriate details of these purposes in our privacy information for individuals?	Appropriate details of the purposes for processing special category and criminal offence data are included in our privacy information for individuals. This is achieved through: • The **Merseyside Police Privacy Notice** published on our website • **APD and DPIA** on the force's website. • **Signage** at ingress and egress points where LFR is deployed. • **Public communications** via website, social media, prior to deployments. These measures ensure individuals are informed about why their data may be processed, the lawful basis, and the safeguards in place.
If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?	We will not use LFR data for any non-policing purpose (e.g., marketing). If a new policing purpose is proposed, it must be legally justified, documented, and explained to the public.

Principle (c): Data Minimisation We only process the minimum amount of data needed to achieve our policing purpose. If you're not on the watchlist, your image is deleted immediately.	
Question	Details
Do you keep images of people who aren't on the watchlist?	No. If you don't match the watchlist, your image is deleted immediately. CCTV footage (where recorded) Retained in line with standard force policy (typically 31 days), subject to CPIA and MOPI requirements
How do you decide who goes on the watchlist?	Watchlists only include people who meet strict legal criteria (e.g., persons wanted on warrant, unlawfully at large, subjects of court orders, high harm suspects, and missing/vulnerable persons for safeguarding). Each deployment is authorised and watchlists are reviewed and trimmed before and during use.
Do we review watchlists regularly?	Yes. We remove anyone who no longer meets the inclusion criteria.
If we plan to use personal data for a new purpose (other than a legal obligation or function set	Information is not used for a different purpose.

out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?	

Principle (d): Accuracy We must make sure the data we use is accurate. LFR alerts are checked by trained officers before any action is taken.	
Question	Details
How do you make sure LFR is accurate?	Our LFR supplier algorithms have been independently tested. We require trained human verification for every alert before any action. We monitor false alerts and demographic performance to continually improve accuracy and fairness.
Do we check matches before acting?	Yes. Every alert is verified by a trained officer before any enforcement action is taken.
What happens if LFR makes a mistake?	False alerts are recorded and reviewed to improve system performance. Officers never act solely on an automated match—human judgment is always applied.
Do we learn from mistakes?	Yes. False alerts are recorded and reviewed to improve system performance.

Principle (e): Storage Limitation We only keep data for as long as necessary. Non-matching images are deleted immediately, and watchlists are regularly reviewed.	
Question	Details
How long do you keep LFR data?	If you don't match the watchlist, your biometric template is deleted immediately. Where an alert is generated and reviewed, we retain only the minimum necessary record for audit and outcome; CCTV footage where used follows standard retention, 31days.
Do you review watchlists?	Yes. Watchlists are regularly reviewed to remove individuals who no longer meet the inclusion criteria, ensuring data is not kept longer than necessary.
Do we audit retention regularly?	Yes. We carry out audits to ensure timely deletion.

Principle (f): Integrity and Confidentiality We keep LFR data secure and confidential. Only authorised officers can access it, and systems are regularly audited.	
Question	Details
Is LFR data secure?	Yes. All data is encrypted and stored on secure police systems that meet national security standards.

Who can access LFR data?	Only authorised officers with appropriate training and clearance. Access is restricted, logged and we carry out regular audits and reviews to check compliance and identify improvements.
Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?	Yes. We have carried out a Data Protection Impact Assessment (DPIA) to identify and understand any risks to people's data. This assessment helps us decide what security measures are needed to keep the data safe. Based on the DPIA, we apply strong safeguards such as encryption, strict access controls, and audit logs so only authorised staff can access the information.
How does Merseyside Police respond to requests about whether an individual is on an LFR watchlist?	Merseyside Police applies the NCND principle when responding to requests about sensitive operational information, such as whether an individual is included on an LFR watchlist. Confirming or denying the existence of such information could compromise policing tactics, ongoing investigations, or public safety. Therefore, where appropriate, Merseyside Police will respond in a manner that neither confirms nor denies the existence of specific data, in line with national policing guidance and Freedom of Information principles.

Further Safeguards

To ensure Live Facial Recognition (LFR) is used responsibly and proportionately, Merseyside Police applies additional measures beyond the core data protection principles:

- **Independent oversight and governance** – All deployments are subject to internal governance and external scrutiny to maintain accountability and public trust.
- **Data Protection Impact Assessments (DPIAs)** – Comprehensive DPIAs are completed and regularly reviewed to assess risks and ensure compliance with legal and ethical standards.
- **Public information on deployments** – We provide clear, accessible information about when and where LFR is used, including signage at deployment sites and updates on our website, so the public can make informed choices.
- **Independent testing & fairness**
  Our LFR supplier algorithms have been tested independently; we provide public information on accuracy and fairness (e.g., false alerts and demographic performance), and we require trained human verification for every alert before action
- **Review cycle**
  We review this APD and related LFR documents at least annually and update our website with changes and upcoming deployments.

These safeguards demonstrate our commitment to transparency, accountability, and the protection of individual rights.

Version History

Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1	06/12/2025	Document Created	Ch/Supt Thornton	Sgt 7649 Hilton

If you need this information in an accessible format, please contact us via our website or call 101