



## Appropriate Policy Document: Live Facial Recognition Compliance with Part 2 of the Data Protection Act 2018 – General Processing

**OFFICIAL**

<b>Publication Scheme</b>	<b>Government Security Classification Scheme (GSCS):</b> OFFICIAL <i>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.</i>  <b>Publish on External Force Website? - Yes</b>
<b>Department of Origin</b>	Matrix Force Operations
<b>Policy Holder</b>	Chief Supt Zoe Thornton
<b>Policy Author</b>	Sgt Chris Hilton
<b>Data Protection Officer</b>	Ian Boyham
<b>This Version</b>	1
<b>Date Created / Modified</b>	06/12/2025
<b>Review By (3 years)</b>	

### Objective

The law requires us to have an Appropriate Policy Document (APD) when we process sensitive data (such as biometric facial data). This document explains how Merseyside Police uses Live Facial Recognition (LFR), what data we process, and how we comply with data protection rules to protect your privacy

### Compliance with Part 2 of the Data Protection Act 2018 – General 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	Retention
Data revealing race or ethnic origin	<input type="checkbox"/>		
Data revealing political opinions	<input type="checkbox"/>		
Data revealing religious or philosophical beliefs	<input type="checkbox"/>		
Data revealing trade union membership	<input type="checkbox"/>		
Genetic data	<input type="checkbox"/>		
Biometric data (used for identification purposes)	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>		
Data concerning a person's sexual orientation	<input type="checkbox"/>		

Criminal Offence Data	Indicator X	Description of Data
Criminal Activity	<input checked="" type="checkbox"/>	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Allegations (including unproven allegations)	<input type="checkbox"/>	
Criminal Investigations	<input checked="" type="checkbox"/>	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Proceedings	<input checked="" type="checkbox"/>	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Offences	<input checked="" type="checkbox"/>	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Criminal Penalties/Sanctions/Fines	<input checked="" type="checkbox"/>	The image reference database will contain images of individuals previous arrested by Merseyside Police and taken into custody
Information about the absence of convictions	<input type="checkbox"/>	
Conditions or restrictions laced on an individual as part of the criminal justice process	<input checked="" type="checkbox"/>	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.	<input type="checkbox"/>	
--	--------------------------	--

## 2. Schedule 1 DPA 2018 Condition for Processing

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

<b>Schedule 1 Conditions Indicator</b> Sensitive processing of biometric data for law enforcement purposes is carried out under the conditions set out in <b>Schedule 1 of the Data Protection Act 2018.</b>	Indicator "x"	Description of Data
<b>Part 1 – Conditions relating to Employment, Health and Research</b> [Insert relevant condition(s) here, e.g., "Processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law for law enforcement purposes."]	<input type="checkbox"/>	
<b>Part 2 – Substantial Public Interest Conditions</b> Processing is necessary for reasons of substantial public interest, specifically:		
Preventing or detecting unlawful acts [10]	<input checked="" type="checkbox"/>	Biometric data (facial images) and associated identifiers used to identify individuals involved in criminal activity or wanted by police.
Protecting the public against dishonesty, malpractice, or other improper conduct [11]	<input checked="" type="checkbox"/>	Facial recognition data linked to persons suspected of fraud, dishonesty, or other improper conduct impacting public safety.
Preventing fraud [12]	<input checked="" type="checkbox"/>	Facial images and watchlist data used to identify individuals suspected of fraudulent activity.
Safeguarding of children and individuals at risk [18]	<input checked="" type="checkbox"/>	Facial recognition data used to locate missing persons, vulnerable individuals, or those at risk of harm.
<b>Part 3 – Additional Conditions relating to Criminal Convictions</b> Processing of criminal offence data is carried out under the conditions set out		

in <b>Schedule 1, Part 3 of the Data Protection Act 2018.</b>		
Statutory etc. and government purposes [36]	<input checked="" type="checkbox"/>	Criminal offence data relating to individuals wanted by police, subject to court orders, or linked to law enforcement intelligence.
Administration of justice [37]	<input checked="" type="checkbox"/>	Data used for the prevention and detection of crime and supporting criminal investigations.

### 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**

<b>Principle (a) Lawfulness, fairness and transparency</b>	
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 an appropriate lawful basis for processing and a further Schedule 1 condition for processing special category/criminal offence data?	<b>Lawful Basis and Conditions</b> <ul style="list-style-type: none"> <li>• <b>Lawful Basis:</b> Section 35(2) DPA 2018 – Processing is necessary for law enforcement purposes.</li> <li>• <b>Special Category Data Condition:</b> Schedule 1, Part 2 – Substantial Public Interest (Paragraphs 10, 11, 14, 18).</li> <li>• <b>Criminal Offence Data Condition:</b> Schedule 1, Part 3 – Statutory and government purposes (Paragraph 36) and Administration of justice (Paragraph 37).</li> </ul>
Do we make appropriate privacy information available with respect to the special category/criminal offence data?	Merseyside Police makes appropriate privacy information available regarding the processing of special category and criminal offence data for Live Facial Recognition (LFR). This includes: <ul style="list-style-type: none"> <li>• <b>Privacy Notice</b> published on the Merseyside Police website: [</li> <li>• <b>Signage</b> at ingress and egress points of each location covered by LFR cameras</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Public communications</b> via website, social media, and media outlets prior to deployments</li> <li>• <b>Stakeholder briefings</b> and community engagement sessions</li> <li>• <b>Reference to Data Protection Impact Assessment (DPIA):</b></li> </ul> <p>These measures ensure compliance with the transparency principle and allow individuals to understand how their data is processed.</p>
Are we open and honest when we collect the special category/criminal offence data and do we ensure we do not deceive or mislead people about its use?	<p>Yes. Merseyside Police is committed to being open and transparent when collecting and processing special category and criminal offence data through Live Facial Recognition (LFR). We ensure that:</p> <ul style="list-style-type: none"> <li>• <b>Signage</b> is displayed at ingress and egress points of each location covered by LFR cameras.</li> <li>• <b>Public notices</b> are published on the Merseyside Police website and social media prior to deployments.</li> <li>• <b>Media communications</b> inform the public about intended deployments, particularly for large events.</li> <li>• <b>Privacy Notice</b> and <b>Data Protection Impact Assessment (DPIA)</b> are available online for review.</li> <li>• Stakeholder engagement sessions are held to explain the technology, governance, and safeguards.</li> </ul> <p>We do not deceive or mislead individuals about the use of LFR. All communications clearly state the purpose of processing, the lawful basis, and the safeguards in place.</p>

### 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
Have we clearly identified our purpose(s) for processing the special category/criminal offence data?	<p>The purposes for processing special category and criminal offence data have been clearly identified and documented. These purposes are set out in the Data Protection Impact Assessment (DPIA) and Policy Documents. This APD references those documents rather than duplicating the content.</p>
Have we included appropriate details of these purposes in our privacy information for individuals?	<p>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:</p> <ul style="list-style-type: none"> <li>• The <b>Merseyside Police Privacy Notice</b> published on our website</li> <li>• <b>APD and DPIA</b> on the force's website.</li> <li>• <b>Signage</b> at ingress and egress points where LFR is deployed.</li> <li>• <b>Public communications</b> via website, social media, prior to deployments.</li> </ul> <p>These measures ensure individuals are informed about why their data may be processed, the lawful basis, and the safeguards in place.</p>
If we plan to use personal data for a new purpose (other than a legal	<p>We will not use LFR data for any nonpolicing purpose (e.g., marketing). If a new policing purpose is proposed, it must be legally justified, documented, and explained to the public.</p>

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?	
--	--

### 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, highharm suspects, and missing/vulnerable persons for safeguarding). Each deployment is authorised and watchlists are reviewed and trimmed before and during use.
How do you ensure that images included in LFR watchlists are appropriate and meet quality standards for accurate matching	All images included in LFR watchlists must meet defined quality standards to ensure accurate matching. Images should be clear, recent, and suitable for biometric comparison. Poor-quality or outdated images will not be used and will be removed during watchlist review prior to deployment.
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?	Information is not used for a different 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, 31 days.
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.

### 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 rationale 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