

# Data Protection Legislation

Appropriate Policy Document (APD)

Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 Data Protection Act 2018

Essex Police Live Facial Recognition (LFR)

Processing biometric data, for the purpose of uniquely identifying an individual.

October 2023

Version 1.0

## Version Control

Version	Date	Author	Purpose
V1.0	12/10/2023	Scott Ashby	

## Introduction

This policy document has been produced in accordance with Essex Police' obligations under Part 3 of the Data Protection Act 2018 (DPA). It should be read alongside the Essex Police Privacy Notice. Data protection policy specific to LFR is also to be found in the LFR Policy and Data Protection Impact Assessment (DPIA) and the Part 2 DPA 2018 and Article 9 GDPR.

Sections 35(3), 35(5)(c) and 42 Part 3 of the DPA 2018 set out the requirement for an APD to be in place when conducting sensitive processing of personal data for Law Enforcement (LE) purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to GDPR special category data. Sensitive processing includes: -

- a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- c) the processing of data concerning health;
- d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. In addition, you may only process sensitive personal data for LE purposes if you have an APD, and if the processing: -

- is based on the consent of the data subject - section 35(4);
- or
- is strictly necessary for the LE purpose and is based on a Schedule 8 condition - section 35(5).

## This Policy Document

This document will demonstrate that the processing of this sensitive data is compliant with the requirements of Part 3 section 42 of the DPA.

## Description of Data Processed

The sensitive data processed utilising LFR: -

- Biometric data for the purpose of uniquely identifying an individual.

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

The watchlist for LFR is primarily a subset of the Essex Police custody image dataset but may also include other lawfully held images.

All watchlist images will have a biometric template created (sensitive personal data) at the point of enrolment to the FRT system.

All faces compared against the watchlist have a biometric template created (sensitive personal data).

Biometric data used to uniquely identify an individual is considered to be sensitive personal 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 individual permanently deleted once this comparison has been completed. No other personal identifiers are collected in addition to the biometric image.

Essex Police is not relying on consent for processing.

### **Conditions for processing sensitive data.**

There are a number of relevant conditions in Schedule 8 which will apply for use of LFR, which apply to current policing practices in any event:

#### 1. Statutory etc. purposes

This condition is met if the processing—

- (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
- (b) is necessary for reasons of substantial public interest.

The police have a common law duty to prevent and detect crime: 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 prevention and detection of crime and the safety of the public. In determining necessity, Essex 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.

Condition 1 is the primary condition relied upon. However, there are other Schedule 8 conditions which may also apply:

## 2. Administration of justice

This condition is met if the processing is necessary for the administration of justice.

E.g. The identification of individuals who are evading justice having committed a criminal offence or who are interfering with the administration of justice

## 3. Protecting individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or another individual.

E.g. Where it is necessary to assess the immediate danger to officers or other individuals by establishing if there is a known history of violence.

## 4. Safeguarding of children and of individuals at risk

This condition is met if-

(a) the processing is necessary for the purposes of-

- (i) protecting an individual from neglect or physical, mental or emotional harm, or
- (ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is-

- (i) aged under 18, or
- (ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

Please refer to the Data Protection Act 2018 for the full provisions of this condition.

E.g. processing of images of persons believed to be missing persons.

## 8. Preventing fraud

(1) This condition is met if the processing-

- (a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and
- (b) consists of-

- (i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,

- (ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or
  - (iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).
- (2) In this paragraph, “anti-fraud organisation” has the same meaning as in section 68 of the Serious Crime Act 2007.

E.g. processing images for persons suspected of committing a fraud offence.

## **Procedures for ensuring compliance with the DPA principles**

### **Accountability Principle**

Essex Police have put in place appropriate technical and organisational measures to meet the requirements of accountability and demonstrate compliance with wider requirements of Part 3 of the DPA 2018 and in particular the principles. These include: -

- The appointment of a data protection officer who is responsible for data protection compliance for LFR.
- Taking a ‘data protection by design and default’ approach to our activities.
- Maintaining documentation of our processing activities specifically with reference to section 61 and 62 DPA 2018.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out DPIA’s for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

### **Principle (1): lawfulness and fairness**

Processing personal data must be lawful and fair. 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 is necessary for the performance of a task carried out for that purpose by Essex Police as a competent authority. As LFR involves sensitive processing, in addition, in the absence of consent, it is only lawful if the processing is strictly necessary for the LE purpose and the processing meets at least one of the conditions in Schedule 8 and Essex Police has in place this APD.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff 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. Relevant documentation and additional information about how LFR is used is available to the public on the Essex Police website, facial recognition section.

The processing of data by LFR is strictly necessary for the exercise of Essex Police' functions of preventing and detecting crime and protecting public safety for reasons of substantial public interest (see above under **Conditions for processing sensitive data**). Reliance will be primarily on condition 1 of Schedule 8, but conditions 2, 3, 4 and/or 8 may also apply. We have given examples of where this may be the case above. Essex Police will always consider whether the use of LFR is strictly necessary (i.e. taking into account consideration of other measures not involving sensitive processing and whether they could achieve the same outcome) and will ensure that at least one relevant condition is satisfied.

### **Principle (2): purpose limitation**

Essex Police' LE purposes for processing using LFR are primarily the prevention, investigation, detection and prosecution of crime but also the safeguarding against and the prevention of threats to public security. These are all LE purposes under s.31 DPA 2018.

On each occasion that LFR is used, the relevant specific and legitimate LE purpose will be explicitly recorded.

We process sensitive data using LFR when it is necessary for us to fulfil these statutory functions listed above in the substantial public interest, including where it is necessary for complying with or assisting another body to comply with a regulatory requirement, to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts, or for disclosure to elected representatives. An example would be if an individual is suspected of committing a criminal offence.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other LE purposes here, providing the processing is necessary and proportionate to that purpose. This means that in particular we consider what we seek to achieve, whether there are alternative measures which would not involve sensitive processing but which would achieve substantially the same outcomes, and the same or lesser impact on individuals and the community.

If we are sharing data collected for LE purposes with another controller, we will document that they are authorised by law to process the data for their LE purpose and that the processing is necessary and proportionate to that purpose.

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

We will not process data collected for an LE purpose for a purpose that is not an LE purpose unless the processing is authorised by law and meets the requirements of the UK-GDPR and DPA.

### **Principle (3): data minimisation**

We process personal data necessary for relevant LE purpose and ensure it is adequate, relevant and not excessive in relation to the purpose for which it is processed. The information we process is only that which is necessary for and proportionate to our purpose. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. An example would be if another individual's image was captured that was not subject to an enquiry.

In addition, we 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 database.

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.

#### **Principle (4): accuracy**

We will retain the probe image of the individual and biometric template for no longer than is necessary for the LE purpose for which it is processed. The source system (Athena) 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 consideration will be undertaken by an LFR Operator. Where we 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, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision and take appropriate steps to inform the data subject. Where we erase or rectify personal data we will inform any recipients with whom we have shared that data.

#### **Principle (5): storage limitation**

All sensitive data processed by us for the purpose of an LE purpose is retained for the periods set out in our retention schedule. 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. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

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 a data sharing agreement 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.

### **Principle (6): integrity and confidentiality (security)**

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

Our 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 sign 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.

All staff receive basic data protection training 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

The systems we use to process personal data allow us respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information 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.

## **Retention and Erasure**

### **Particular to LFR Application**

- where the LFR application does not generate an alert, then a person's biometric template and probe image is immediately automatically deleted.
- 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.
- 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.
- watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.
- LFR operator and engagement logs are retained in line with MOPI retention periods



All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or*
- in accordance with Essex Police complaints / conduct investigation policies.

### **Source System – Athena**

Please refer to Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4)

Non-conviction – upon request

Group 1 or 2 (Public Protection Matters & sexual, violent or other serious offences respectively) – 10 years upon request then review

Group 3 (all other offences) – 6 years upon request then review

Group 4 (missing persons) – 6 years then review

All other personal data will be stored in accordance with MOPI standards.

Group 1 - subject is 100 years the review

Group 2 – 10 year clear period then review

Group 3 – 6 year clear period

Group 4 (missing persons) – 6 years then review

### **Appropriate Policy Document review date**

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.


This policy will be reviewed annually or revised more frequently if necessary.

Account is taken of all regulatory and policing information and guidance, relevant case law and changes to legislation.

A copy of this policy will be published on the Essex Police website and a copy is available to the Information Commissioner, on request, free of charge in accordance with s42(3)(c) DPA.

### **Policy document Sign-Off**

<b>Person completing the APD</b>	Name (in capitals)	<b>SCOTT ASHBY</b>
	Date:	<b>11/10/2023</b>
<b>Data Protection Officer</b>	Name:	<b>Michelle WATSON</b>

	Date:	<b>11/10/2023</b>
<b>Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))</b>	Signed:	
	Name (in capitals)	<b>ANDREW PRTICHARD ACC 10005</b>
	Date:	<b>13/10/23</b>