Data Protection Impact Assessment (DPIA) – Stage 1

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material available before completing the form.

Data Protection Impact Assessment (DPIA)		
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.		
Section 1 - Governance		
Project Proposal Name:	Live Facial Recognition	
Project Sponsor:	ACC Simon Wilson	
Information Asset Owner(s):	DCS Morgan Cronin	
DPIA Advisor:	Michelle Watson	
Date on which processing will commence:	12/08/2024	
Date submitted to DPIA Advisor:	29/07/2024	
Note: DPIA Advisor will endeavour to give an **initial response** within 10 working days of receiving the completed form.		
DPIA Assessment		
*****DPIA ADVISOR USE ONLY*****		
A. DPIA is not required.	☐	**DPO Comments:** **RM Comments:**
B. DPIA is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	☐	**DPO Comments:** **RM Comments:**
C. DPIA is required.	☒	**DPO Comments:** 29/07/2024 A full DPIA2 is required. This processing involves a number of the areas deemed as potentially high-risk processing to the rights and freedoms of data subjects and as such a full DPIA must be undertaken. **RM Comments:**

Section 2 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

Live Facial Recognition (LFR) is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces against a predetermined watchlist and generates an alert when a possible match is found.

LFR can be a valuable policing tool that helps forces keep the public safe and to meet their common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

The following are illustrative examples where LFR may assist Essex Police achieve their policing purposes:

- Supporting the location and arrest of people wanted for criminal offences.
- Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders).
- Supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc).
- Supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

The technical operation of LFR comprises of the following six stages:

Compiling/using existing database of images: the LFR application requires a watchlist of reference images against which to compare facial images from the video feed. For images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a biometric template).

The Essex Police LFR policy outlines considerations relevant to lawfully compiling a watchlist including determining which persons may be on a watchlist and the sources of watchlist imagery.

Facial image acquisition: a CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the zone of recognition and using it as a live feed. The siting of the CCTV cameras, and therefore the LFR deployment location is important to the lawful use of LFR. The Essex Police LFR policy and standard operation procedure (SOP) provide considerations relevant to the locations Essex Police may select to deploy the cameras when using them for LFR.

Face detection: Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

Feature extraction: Taking the detected face the software automatically extracts facial features from the image, creating the biometric template.

Face comparison: The LFR software compares the biometric template with those held on the watchlist.

Matching: When the facial features from two images are compared the LFR application generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

Watchlists

The watchlist is bespoke for every deployment and the rationale for the make-up of the watchlist must be intelligence-led, justified, proportionate and necessary, with the nature of the watchlist recorded prior to each deployment.

The candidate images and related biometric template are deleted immediately post deployment and in any case within 24 hours.

The criteria for constructs of watchlists for use with LFR must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. Watchlists, and any images for inclusion on a watchlist, must also be limited to the categories of image articulated in Force policy documents which are images of people who are:

a. wanted by the courts; and/or
b. suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
c. subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or
d. missing persons deemed increased risk; and/or
e. presenting a risk of harm to themselves or others.

The inclusion in a watchlist will be deemed strictly necessary to achieving the policing outcome and only when less intrusive means of location have proved unsuccessful.

Each deployment of Live Facial Recognition will be subject to a full Authorising Officer pre-deployment authorisation report which will clearly define the strictly necessary argument for

processing personal data, along with setting out clearly the case for the deployment's compliance with the College of Policing's Authorised Professional Practice of being targeted, intelligence led and time bound and geographically limited. That document should be read in conjunction with this DPIA for a full understanding of the specific processing, risk assessment and mitigations applied.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

Personal data which is already accessible and processed by the police (images held in Athena by example) will be processed in conjunction with the use of LFR.

This information will be added to a watchlist and uploaded onto live facial recognition software. For images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a biometric template).

CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the zone of recognition. The LFR software then detects individual human faces, and automatically extracts facial features from the image, creating a biometric template.

The LFR software then compares the biometric template with those held on the watchlist. If there is a match, the LFR system will create an alert, resulting in police personnel checking the images to see if they match. If they do, an officer(s) will be sent to engage with the person identified.

Data associated with the person from the watch list, which may include but is not limited to, their name, date of birth and address of an individual, will not be included in the actual LFR deployment of facial recognition technology but would be processed in the event of a possible match.

LFR overall deployment will involve various categories of personal data including biometric data for the LFR software, however names, DOB's, addresses, criminal offence data may be recorded as part of the deployment with data subjects matched and engaged by police. The data will be processed both in relation to those entered onto the watchlist and of those data subjects passing the zone of recognition of the CCTV camera although not all data sets will be captured for all, i.e. name, address, DOB etc are only relevant to those data subjects on the watchlist, and who officers will engage with if matched. Those data subjects who pass the zone of recognition but are not subject of the watchlist will have their images deleted immediately.

2.3 Will special category data be used in the proposal? (Select all that apply)

☒ Race	☐ Trade union membership
☒ Ethnic origin	☐ Genetic Data
☐ Political opinions	☒ Biometric Data
☐ Sex life	☐ Sexual orientation
☐ Religion	☐ Health

☐ Philosophical beliefs ☐ None

The LFR application does not process specific data related to race or ethnic origin however, due to public interest in the system and the use of images to create a watchlist, then Essex Police have recognised this special category data here to ensure additional recognition and protection of the rights and freedoms of data subjects in these categories.

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in the force's possession, from a partner agency.

CCTV cameras deployed will capture images / biometric data of people walking past the camera zone of recognition. Live facial recognition software will then compare that biometric data to the data on the watchlist which is compiled from data already held by Essex Police through lawfully held images such as custody images.

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

The data obtained will be automatically cross referred against a pre-prepared watchlist as explained in 2.1. All other biometric data captured will be deleted immediately. The CCTV feed will be deleted within 31 days.

2.6 How many individuals will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects

☐ 100 to 1000 data subjects

☒ 1000 to 5000 data subjects

☐ More than 5000 data subjects

☐ Unable to determine

2.7 What categories of data subject are involved? (Please select all applicable categories below)

☒ Persons suspected of having committed or being about to commit a criminal offence

☒ Persons convicted of a criminal offence

☒ Persons who are or may be victims of a criminal offence

☒ Witnesses or other persons with information about offences

☒ Children or vulnerable individuals

☒ Police officers or staff (current and former)

☒ Other

If other then please provide further details below:

Deployments will be a real time capture of the biometric templates of individuals who cross the path of the camera therefore a cross section of the general public including all categories will potentially be processed.

The watchlist will be compiled from lawfully held images based on the criteria for the deployment.

It is possible that the personal data of individuals aged under 18 years, those under 13 years, a person with a disability or vulnerable adults will be processed where there is a policing need, and it is deemed to be necessary and proportionate to locate and/or safeguard these individuals.

2.8 Will it involve the collection of new information about individuals? Will the force collect data that it has not previously collected or had access to?

☒ Yes
☐ No

The capture of biometric data of data subjects passing the zone of recognition does ultimately mean that the force will be processing data it has not previously collected however, where a data subject is not matched with those on the watchlist, the image is deleted immediately.

2.9 Data Sharing **Does the processing involve:**		**Select one option**
2.9.1	Data being shared with third parties external to the force or recipients that have not previously had routine access to the information?	☐ Yes ☒ No
2.9.2	Transferring data outside the UK but within the EU?	☐ Yes ☒ No
2.9.3	Transferring data outside the EU?	☐ Yes ☒ No
2.9.4	Storing data using a cloud service provider?	☐ Yes ☒ No
2.9.5	Is there a data processing contract, or information sharing agreement in place with all parties with whom data will be shared?	☒ Yes – agreements in place via contractual clauses ☐ Not yet – agreements required ☐ No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?
For example, can the aim be achieved by using less data or different types of data?
Are all categories of data necessary to achieve the aim?

LFR can be a valuable policing tool that helps police forces keep the public safe and to meet their common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

The following are illustrative examples where LFR may assist Essex Police achieve their policing purposes:

a. Supporting the location and arrest of people wanted for criminal offences.
b. Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders).
c. Supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons deemed at increased risk, etc).
d. Supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them.

The challenges presented in locating and arresting offenders should rightly be challenged and with the assistance of technology, more enhanced and cost-effective methods can be called upon to bring those responsible or suspected of offences more quickly to justice.

Those data subjects added to a watchlist will be subject to strict criteria as set out in the Essex Police policy, and where less intrusive means have proven unsuccessful. The deployment and location will be determined by there being reasonable grounds to suspect that the proposed deployment location is one at which one or more people on the watchlist will attend at a time, or times, at which they are to be sought by means of LFR.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal.
Weigh the advantages of achieving your purpose against disadvantages to data subjects.

As explained above LFR can have a significant impact in helping the Essex Police achieve their policing purpose by supporting police to arrest those wanted for serious offending, for those who mean to cause serious harm and for those who may be at high risk of harm themselves.

Essex Police understands that LFR is a new technology and there may rightly be concerns from data subjects as to the intrusiveness of the technology. For those not on the watchlist who are in an area where LFR is deployed there will be no impact and minimal intrusiveness except where there is an alert, whereby an officer will compare the images and if necessary, can speak with the identified individual. The signage and information around the target location means that individuals can choose not to be in the vicinity of the LFR technology. For those not on the watchlist who do have their biometric data captured, the data is deleted immediately.

Section 3 – Lawful Basis
3.1 Lawful Basis To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.
Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes): Necessary for a law enforcement purpose Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes): Necessary for the performance of a task carried out in the public interest or in the exercise of official authority
3.2 Further Special Category Lawful Basis If processing special category data (section 2.3) you must have identified a further lawful condition
Operational Data: The processing is strictly necessary (please tick to confirm) ☒ **AND** One of the following conditions applies (select from the list): Statutory Purpose
Administrative Data It is necessary for one of the following conditions (select from the list): Choose an item. **OR** It is in the substantial public interest (tick to confirm) ☒ **AND** for the following purpose: Statutory function
The Essex Police Appropriate Policy Document (APD) sets out how Essex Police complies with data protection legislation in the processing of sensitive and special category data for both law enforcement and general purposes.
Section 4 – Record Review, Retention and Disposal
4.1 Does the proposal have a review, retention and disposal process that complies with Force Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within W 1012 Procedure/SOP – Records Review, Retention & Disposal.
☒ Yes ☐ No The Essex Police Appropriate Policy Document (APD) and the Force Policy outlines the retention policy.

4.1.1 Is this a new system or an update to an existing one?	☒ New ☐ Update

4.1.2 If this is a new system, how is this data currently recorded or captured? (E.g., in paper format, on a different system etc) This data may not currently be captured via a different method.	This is a new system to Essex Police. We will use existing images available to Essex Police from Athena and other police systems to create the watchlist. The data generated by LFR software is not currently captured. We have not had this technology to utilise previously (other than to trial the technology) therefore, traditional policing investigation techniques are currently used to locate those that may be added to watchlist. The EP policy setting out the criteria for being added to a specific watchlist would ensure that there is an assessment of proportionality and necessity will be undertaken before inclusion.
4.1.3 If this is a new system, how are/will any records collected via the old method be managed?	N/A – no records will be collected by an old method.
4.1.4 If this is an update to an existing system, how will the legacy records be managed?	N/A
If the records you are collating relate to crime investigation, please go to Section 4.2. If they relate to a non-crime function, please go to Section 4.3.	
4.2 Records collected are relevant to crime investigation.	☒ Yes
4.2.1 If these records are evidential how will they be retained and potentially disclosed in line with CPIA?	They are not evidential. Any matches between the images captured and the watch list will simply result in an officer approaching the person and conducting a stop check.
4.2.2 What MOPI groups will the records collected be relevant to? (1,2,3 or all)	Biometric data will be immediately destroyed if there is no match to data on the watch list, and within 24 hours if there is a match. 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's complaints / conduct investigation policies.

4.2.3 How are records categorised? For example, is a MOPI grouping selected? Is an offence type selected?	Biometric data will be immediately destroyed if there is no match to data on the watch list, and within 24 hours if there is a match. 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's complaints / conduct investigation policies.
4.2.3 How will each record type be managed on the system? Consider how long the records are retained – are they retained differently according to MOPI group? Will records be reviewed prior to deletion - if so, how do you know when to review them and who will be completing this? Is any deletion of records automated and if so, please explain how this process works?	The LFR application will create biometric templates of the faces in the watchlist. This will then use a live camera feed to scan faces of individuals in a designated area creating biometric templates of each to compare against those in the watchlist. The application 'extracts' a face from CCTV footage and creates a biometric template and then compares it against a pre-defined watchlist. Every candidate image in the watchlist will also have a biometric template created. In doing so, the application does not save the live CCTV feed, only a particular face if a possible match is made against a candidate image along with a wider CCTV frame from which the image was extracted. The CCTV feed will itself be saved for 31 days and then deleted. Not every person that is captured via the CCTV will be enrolled into the application. The face must be of sufficient quality to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include: • crowd density, • individual movements, • face angle; and • lighting. It is the intention during each deployment to allow the LFR application to enrol and therefore process as many individuals as possible, however any processing that does not lead to an alert will be momentary, and the image permanently deleted. No additional information will be

	attributed to the images of individuals enrolled into the LFR application. The application has a built-in audit trail functionality that ensures images that do not generate a possible match against a candidate image are not retained within it. The watchlist is created via a CSV file which is saved in a secure folder along with the corresponding candidate images within the force ICT domain. The content of the folder is extracted into the LFR application prior to deployment via a secure file sharing platform. The maximum retention period for possible match images and the related biometric templates is 24 hours although generally this information is deleted immediately post deployment.
4.2.4 Are there National Police Chiefs Council guidelines for the retention, review and disposal of these records?	No
4.2.5 Is there a force policy or SOP in relation to the management of these records? Please provide relevant policy numbers.	Yes. Force policy has been written. An Appropriate policy document has also been produced to ensure compliance with data protection legislation.
4.2.6 Will any copies of this data be held elsewhere? (For example, paper copies in casefiles, discs etc)	No
4.3 Records collected are not relevant to crime investigation.	☐ Yes
4.3.1 Is there National Guidance, legislation or Force policy/SOP that relates to the retention, review and disposal of these records?	Please see 4.2.5
4.3.2 How will each record type be managed on the system?	Please see 4.2.3
4.3.3 Will any copies of this data be held elsewhere? (For example, paper copies in casefiles, discs etc)	No

Section 5 – ICO: Additional Factors			
The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.			
Does the processing involve:		**Please check either Yes or No**	**If 'Yes' then please provide further details**
5.1	**Systematic, extensive and large scale profiling and automated decision-making about people?** *"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"* Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.	☐ Yes ☒ No	Click here to enter text.
5.2	**Large scale use of special category data or criminal offence data?** *"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"*	☒ Yes ☐ No	Click here to enter text.
5.3	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☒ Yes ☐ No	See section 4.2.3.

5.4	**New technologies or techniques?** *"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"*	☒ Yes ☐ No	Live facial recognition is a relatively new technology in policing.
5.5	**Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?** *"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"*	☐ Yes ☒ No	Click here to enter text.
5.6	**Biometrics/genetic data?** *"Any processing of biometric data"* ***and/or*** *"any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject" Biometric data can include Facial Recognition technology, fingerprints and is defined as*	☒ Yes ☐ No	LFR processes biometric data
5.7	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☒ Yes ☐ No	The LFR application will create biometric templates of the faces in the watchlist. This will then use a live camera feed to scan faces of individuals in a designated area creating biometric templates of each to compare against those in the watchlist.
5.8	**Invisible processing?** *"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"* For example, when gathering data, without the knowledge of the data subject, in the course of a police investigation.	☐ Yes ☒ No	There will be a period of public consultation prior to any deployment as well as clear and overt signage advising members of the public that they are walking into the area scanned by the LFR technology. There is no invisible processing.
5.9	**Tracking?**	☐ Yes	Click here to enter text.

	"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"	☒ No	
5.10	**Targeting of children or other vulnerable individuals?** *"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children* For example, the use of personal data relating to children for the purposes of marketing their online safety products.	☐ Yes ☒ No	Click here to enter text.
5.11	**Risk of physical harm?** *"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".* For example, if data relating to CSAE, HUMINT or protected persons data was compromised then it could jeopardise the safety of individuals.	☐ Yes ☒ No	Click here to enter text.
5.12	**Evaluation or scoring?** *"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of a police recruitment process.*	☐ Yes ☒ No	Click here to enter text.
5.13	**Data processed on a large scale.** *Considerations include:* • *The number of data subjects concerned* • *Volume of data and/or range of data items* • *Duration, or permanence, of the data processing* • *Geographical extent of data processing*	☒ Yes ☐ No	The cameras to be deployed will capture images of people in the designated camera zone. Not every person that is captured via the CCTV will be enrolled into the application. The face must be of sufficient quality to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include:

			• crowd density, • individual movements, • face angle; and • lighting. However, it is impossible to say in advance how many persons may walk in view of the camera
5.14	**Preventing data subjects from exercising a right?** *The rights are:* • *The right to be informed* • *The right to access data* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to object* • *The right to portability* • *Rights relating to automated processing*	☐ Yes ☒ No	Click here to enter text.

Please forward the completed form to the DPIA Advisor;

DPO@essex.police.uk (for Essex Police & SCD) or

information.security@kent.pnn.police.uk (for Kent Police & SSD).