Data Protection Impact Assessment (DPIA) – Stage 2

In this stage of the DPIA process you must provide full details about the lifecycle of the data and the risks associated with the proposal. The information you provide will supplement the information provided in Stage 1.

The aim of this process is to identify and mitigate risks. If any **residual risks** to individuals are **high** then the ICO must be consulted before processing commences.

Section 6 - Impact
Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: the force; the data subjects; and society/the general public Describe the benefits and disadvantages to each of the above.
The technical operation of LFR comprises the following six stages: (1) Compiling/using an existing database of images. LFR requires a database of existing facial images (referred to in this case as a watchlist) against which to compare facial images and the biometrics contained in them. For such 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. (2) Facial image acquisition. A CCTV camera takes digital pictures of facial images in real time. This case is concerned with the situation where a moving image is captured when a person passes into the camera's field of view, using a live feed. (3) Face detection. Once a CCTV camera used in a live context captures footage, the software: (a) detects human faces and then (b) isolates individual faces. (4) Feature extraction. Taking the faces identified and isolated through face detection, the software automatically extracts unique facial features from the image of each face, the resulting biometric template being unique to that image. (5) Face comparison. The LFR software compares the extracted facial features with those contained in the facial images held on the watchlist. (6) Matching. When facial features from two images are compared, the LFR software generates a similarity score. A threshold value is fixed to determine when the software will indicate that a possible match has occurred. Where an individual is engaged by an officer following a possible match other details such as their name may be captured however this is out of scope of the LFR activity. **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 specific criteria for identification of the watchlist for the trial deployment is noted in the authorising officer policy document.

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 (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.

Impact on force
The deployment of LFR can be a valuable policing tool that help the forces keep the public safe and to meet our common law policing duty, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

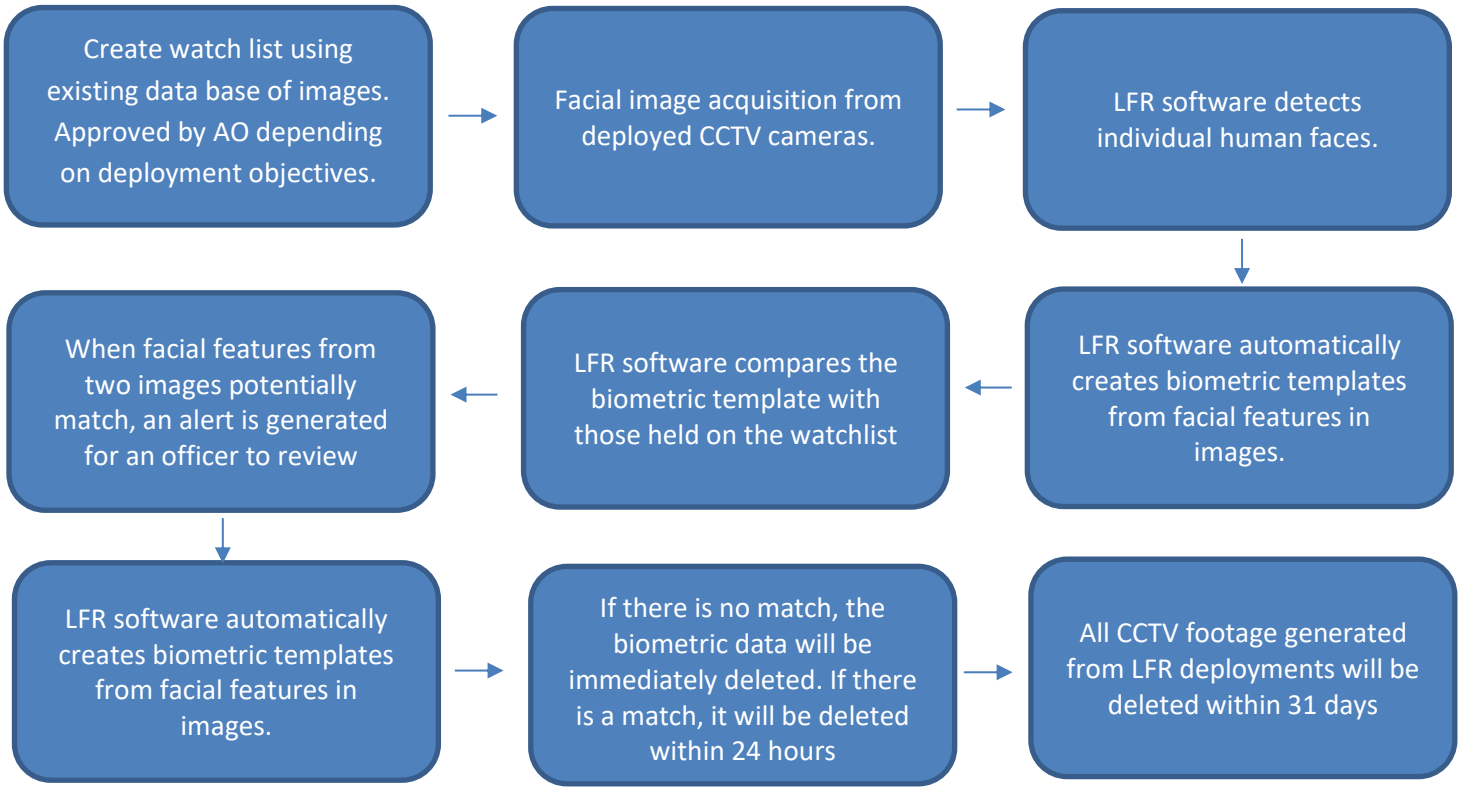
Impact on data subjects
Should a person on the watchlist enter an LFR deployment area and an alert be generated, an officer will compare the images and if necessary, officers will speak with the identified individual. For those not on the watchlist who are in an area where LFR is deployed there will be minimal impact or intrusiveness as their biometric data will be briefly checked and deleted.

Impact on the public
There is an expectation on Essex Police to bring offenders to justice, reduce criminality and make the Essex Policing area a safer place for people to live, work and visit. LFR technology allows Essex Police to achieve those aims, but only where there is targeted, intelligence-led and both time and geographically limited rational for doing so, ensuring that the argument for it being strictly necessary to process data in this way is met.

Section 7 - Information Lifecycle

7.1 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.



7.2 Provide a full description of the information lifecycle	
Stage of Processing	**Description**
Collection Where does the data originate from, who will collect it, how will it be data obtained and how often?	The LFR application requires a watchlist of reference images against which to compare facial images from the video feed. These images will be obtained from existing Essex Police images from Athena, such as custody images. 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. CCTV cameras deployed at an agreed location for a specific policing purpose as declared by the AO pre-deployment document, will capture digital pictures of facial images in real time of persons passing the camera locations. LFR software will detect facial images and automatically cross refer the biometric data to the data on the

	watchlist.
Storage Describe where and how the data is to be stored	The collection of personal information is via two CCTV cameras connected to the standalone laptop/server. The laptop is not connected to the force ICT infrastructure and can be considered a 'black box' solution (an independent system to the current technical EP architecture). The application extracts a face from CCTV footage (known as a probe image) 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 probe image was extracted.
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	When facial features from the watchlist data and the converted CCTV biometric data match, trained members of police personnel will review the alerts and decide 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.
Access Describe who has access to the data throughout the life of the processing	Two types of access will be available to the application – user and administrator access levels. Operating staff will all be vetted and cleared to at least MV/SC level. Access is only granted to users following completion of training. Only those officers involved in the deployment will have access to the personal data relevant to deployment.
Recording Describe the processes for recording the data	CCTV cameras will capture images of people passing the cameras. LFR software will convert the images into biometric data, and will then automatically cross refer this data to the biometric data of images on the pre-prepared watch list.
Processors Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?	There are no third parties involved in the processing. The processing will be take place outside the UK.
Sharing With which external organisation(s) is the data shared, what data is shared, and why?	The data will not be shared with any external organisation unless legally required to do so.

Describe any sharing that will occur within the force. Outline any national and international sharing or processing.	
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate	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. The watchlist data will be deleted within 24 hours.
Disposal Describe the process for disposal of data, including when and how.	As above.
7.3 Assets Describe the assets that you intend to use.	
Hardware	CCTV Cameras, stand alone computer, encrypted USB
Software	Live Facial Recognition Software
Networks	None.
Hardcopy/paper	None.
Any other relevant assets	None.

Section 8 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you should consider consulting them or their representatives.

8.1 Do you intend to consult data subjects?

☐ **Yes**
If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.

☒ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.	The data subjects effected by this proposal will be people who are added to a watchlist for a specific policing purpose, which will generally involve the deployment trying to assist in one of the following: - Locate wanted persons. - Preventing disruption in the area by identifying persons who may cause harm. - Locate people who may pose a risk of harm to themselves of the wider public. - Support targeted preventative policing activity to prevent criminality and disorder. If it were possible to seek the views of these people, this proposed tactic would be negligible. However, all appropriate documentation relating to the deployment of live facial recognition will be published on the Essex Police Website 7 days prior to any deployment. Whilst data subjects cannot be directly consulted with, Essex Police has an independent ethics committee who have reviewed the proposed use of live facial recognition and are supportive of the proposed deployment.

8.2 Consultation Action Log
Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The general public
- Union representatives
- Information Security
- Information Management
- Legal
- Operational Security Advisor (OpSy)
- Partner agencies
- Data processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome

Information Commissioners Office (ICO)			
Essex Police Ethics Committee	10/10/2023 – formal ethics committee meeting	MS Teams Meeting	Ethics committee supportive of deployment of LFR
Information Security	10/10/2023	Data Protection Officer consulted with Information Security for assessment.	All security aspects covered and approved.
Data Protection Officer	10/10/2023	Reviewed DPIA 1 & 2	DPIA 1 and 2 approved
Legal Services			

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10 i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Examples of **risks to individuals** include**:** • Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights	Examples of **corporate risks** include: • Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations
You should identify **solutions** such as: • Deciding not to collect certain types of data • Reducing the scope of processing • Reducing retention periods • Taking additional technical security measures • Following approved codes of conduct	 • Restricting access to data • Training staff to understand the risks • Anonymising or pseudonymising the data • Using different technology • Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all force systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to DPIA Advisor.

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
	1 - Rare 2 - Unlikely 3 - Possible 4 - Likely 5 – Almost Certain	*1 - Insignificant 2 - Minor 3 - Moderate 4 - Major 5 - Critical*	*High Medium Low*	*Describe the mitigation and whether it will be implemented*	*Is the risk: - Eliminated - Reduced - Accepted*	*High Medium Low*
As a result of the Watchlist being deleted after 24 hours the force	2	3	L	The watchlist is created from pre-existing information held on	Eliminated	L

may be unable to comply with a subject access request from a data subject resulting in complaints, reputational damage, and potential financial claims.				Essex Police systems. Therefore, if it is deleted and is required, it can be re-created using existing information.		
There is a risk that intervention may take place as the result of a False Alert resulting in reputational damage, potential enforcement action and financial penalties, loss of public trust and increased volumes of complaints.	1	4	M	The AO will set the threshold value at an appropriate level to try and ensure that the chances of a false alert are minimal. Any potentially matches that LFR highlights will be reviewed by police personnel before action taken.	Reduced	L
As a result of the scope of a Deployment there is a risk that fair processing information may not be widely available to members of the public resulting in them not being informed of the processing of their personal data resulting in a potential data breach, increased complaints, court cases, enforcement action and reputational damage	3	3	M	A communications strategy will be in place prior to any Deployment to ensure that all available means of communicating the fact that a Deployment will/is taking place via various channels including digital and physical, and information is available to the public on why Deployments are effective to ensure that individuals and the public are confident that the decisions made to deploy and continue to operate LFR are based on firm evidence and transparent analysis. The use of cameras will also be assessed against the	Reduced	L

				Surveillance Camera Commissioner's Camera Code (as required under s29 of the Protection of Freedoms Act 2021). A specific privacy notice, Data Protection Impact Assessments and deployment locations will be published on the Essex Police website.		
As a result of the nature of LFR there is a risk that deployments may limit or contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law resulting in potential legal challenge, financial claims and increase in complaints.	4	3	M	The assessment prior to any Deployment of LFR will determine whether interference with these rights is necessary, proportionate and lawful and whether there are less intrusive methods which could be employed. Full, robust justification will be documented prior to any Deployment.	Accepted	M
As a result of issues to narrow the scope of the Watchlist there is a risk that the images included for a Deployment may be excessive.	2	2	L	The assessment prior to any Deployment will include the requirements and justification of the inclusion of images in the Watchlist to ensure that the strict necessity threshold is met and there is a reasonable expectation that those individuals will be in the vicinity of the Deployment of LFR.	Eliminated	L

				Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use.		
There is a concern that bias may not be eliminated in the algorithm resulting in a disproportionate number of individuals with protected characteristics being identified in false alerts leading to potential legal challenge, financial claims and increase in complaints.	3	3	M	Assurances around the testing conducted by the software supplier are required in the contract and is continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified as part of the public sector equality duty and through assessment by academic institutions, technology vendors and government opinion. Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented. Equality Impact Assessments will be completed and regularly reviewed against legal developments. Any match against a watchlist will require a review from a trained LFR officer before any engagement ensuring a human assessment	Reduced	L

				before interaction with the public.		
As a result of the wide-ranging capability of LFR to process large amounts of personal data there is a risk that the processing of personal data may be excessive resulting in regulatory action.	3	3	M	The assessments prior to a deployment will consider and document why less intrusive methods are not appropriate and justifying the use of LFR based on intelligence. Stringent RRD processes are in place to ensure there is no retention of non-match data.	Reduced	L
There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action.	2	4	M	An additional legislative safeguard is any covert surveillance / activity will require authority under the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016, or the Police Act 1996 as per arrangements for any covert surveillance. There is no intention for Essex Police to deploy LFR in a covert manor.	Eliminated	L
There is a risk that each deployment and watchlist is not subject to a full assessment documenting the rationale for inclusion of images the who, the scope of the location, duration the where and whether the strictly necessary threshold has been met	1	3	L	Any deployment of LFR requires a suite of documents to be completed prior to any deployment of LFR or as soon as possible in urgent cases. These documents require authority to deploy and documents all justification,	Eliminated	L

resulting in a risk of unlawful processing and breaches of the Data Protection Act 2018 which may lead to financial claims and penalties, court cases.				criteria and detail around necessity, effectiveness, and purpose of deployment to ensure it is targeted; intelligence led and time limited.		
As a result of potential incomplete deletion exercises there is a risk that Watchlists may be compiled using custody images which should have been deleted from police systems in line with established retention and deletion procedures or from images of uncertain provenance where accuracy may be an issue (e.g. sourced from social media) there is a risk that these may lead to an unjustified engagement and potentially cause unwarranted and unjustified damage and distress to individuals.	3	3	M	Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. No engagement will be made without checks being made on possible matches without manual intervention to reduce any damage and distress.	Reduced	L
As a result of different scenarios in which a person may be reported as missing there is a risk that the use of LFR to locate that person may not meet the strict necessity threshold and may be unlawful resulting in potential legal challenge, complaints and financial penalties or regulatory enforcement action.	3	3	M	Where a Deployment is being used to locate a missing person a strict necessity test will be conducted to determine the degree to which the missing person is vulnerable and whether there is sufficient intelligence to indicate that the individual may be in a particular area at a particular time. This	Reduced	L

				will need to be signed off by an officer of the required authority.		
Where the force has not completed an appropriate policy document there is a risk that it will be in breach of section 42 of the Data Protection Act 2018 resulting in potential regulatory enforcement action and/or financial penalties.	1	1	L	Essex Police will have an Appropriate Policy Document in place for the trial deployment and a full published force policy document thereafter.	Eliminated	L
As a result of inconsistent guidance around the use of LFR there is a risk that officers may exercise too much discretion around inclusion in the watchlists and the location of the deployment resulting in excessive and unlawful processing of data which may lead to legal challenge, complaints and potential enforcement action.	2	4	M	A pre-deployment document / policy decision will be written by the AO in advance of any activity taking place. This will clearly outline the reason for deploying in a specific area, which will be intelligence or crime data led. They will also outline their rationale for including persons on the watchlist, which will be for a specific policing purpose as per legislation and force policy.	Reduced	L
There is a risk that officers involved in the Deployment of LFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the Deployment of LFR and potential breaches of the DPA'18 which may result in enforcement	2	2	L	As part of the LFR training appropriate data protection training will be provided.	Accepted	L

action, legal action and financial penalties.						
As a result of lack of training and awareness there is a risk the data entered onto the watchlist is not treated within the correct Government Protective Marking Scheme (GPMS) resulting in adequate protection when handled and potential loss and damage.	2	2	L	All Essex Police staff/ officers are trained in respect of the GPMS/ Government Security Classifications (GSC). Officers compiling watchlists will perform this task in a secure environment to which the public do not have access. All watchlists are appropriately stored prior to the operation and are deleted after the deployment.	Accepted	L
As a result of lack of training and awareness there is a risk that the watchlist or other data generated by the LFR application is unlawfully disclosed to third parties	2	2	L	Officers/Staff compiling the watchlists are briefed in respect of watchlist circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff. Any action following an alert may involve EP working with other police forces, law enforcement bodies and other agencies to assist EP in discharging its common law	Accepted	L

				policing powers. This action will not require the sharing of biometric data but may require EP to share personal data, as it would for any investigation, in accordance with EP's routine sharing arrangements.		
As a result of technical failure there is a risk that the equipment will not function correctly resulting in false alerts or failure to identify possible matches resulting in potential damage and distress or threat risk and harm to others.	2	4	M	All equipment to be used has been trialled and tested. NEC algorithms have also been evaluated by the National Physical Laboratory (NPL), NIST and the Department of Homeland Security and Essex Police acknowledge these findings. An LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of the False Alert Rate to below 0.1% will be present at all Deployments. Essex Police LFR Documents also outline points relating to the LFR application to ensure	Accepted	L

				that it is used in a way that maximises its effectiveness. They also place responsibility on the Silver Commander and LFR Operator to continually monitor and review the system's performance. The Gold and Silver Commanders are obligated to stop the Deployment, should the Deployment fail to meet the requirements of the DPA 2018 at any point. The ongoing effectiveness of Essex Police's use of LFR is reviewed by way of the post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.		
9.2 Data Sharing - including the involvement of other Controllers and Processors						
- What contracts, MOUs etc are in place or may be required? - What measures have you taken place to ensure third parties comply with Data Protection laws?				- What risks are involved with sharing data? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?		

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
No risks identified						

9.3 International Transfers

- Will data be shared with a third party based outside the EU?
- If you will be making transfers, how will you ensure that appropriate safeguards are put in place?

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
No risks identified						

9.4 Additional Risk Factors

Describe any further risks, ensuring that any risks not already identified are included.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
No risks identified						

Section 10 – Operational Data Risks - Additional Risks Relevant to Operational Data Only						
This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**						
10.1 Data Logging Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.						
If the data is processed electronically then will a log be retained of the following actions:						
• **Collection** • **Alteration** • **Consultation** • **Disclosure** • **Combination** • **Erasure**	☒ Yes ☐ No* ☐ Not applicable ***If you answered "no" then you must record this as a risk below.					
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
No risks identified						
10.2 Data Categorisation When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.						
Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:						
• Suspected of having committed, or are about to commit, a criminal offence • Convicted of a criminal offence, • Victims of a criminal offence, • Witnesses to a criminal offence.	☒ Yes ☐ No* ☐ Not applicable If you answered "no" then you must record this as a risk below.					

Choose an item. – Choose an item. – Choose an item.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
No risks identified						

Section 11 – Outcome and Review			
11.1 Outcome			
Item	**Name**	**Date**	**Notes**
Residual risks approved by:	Steve Jennings		
DPIA advice provided by:	Michelle Watson	10/10/2023	
11.2 Review			
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.			
Outline: • Who will be responsible for reviewing the processing • The frequency of review • The date of the next review			
D/Supt Steve JENNINGS to review post trial deployment, thereafter annually or if any element of the processing changes.			