

p

Data Protection Impact Assessment (DPIA)

DPIA Information	
Name (and or project number)	Live Facial Recognition (LFR) Van Deployment – v1.1
Forces involved in Project	Joint
Operational Contact	[redacted]
Information Asset Owner	
Business Contact	
Information Governance Contact	

Document Review Information			
Version History	***Version Date***	***Requestor of Change***	***Summary of Change(s)***
0.1	*12/03/2025*		
0.2	*27/05/2025*		

Introduction

The **Data Protection Impact Assessment (DPIA)** process is an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective consideration where solutions can be more costly or delay implementation. A DPIA, can also identify whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way the forces use individual's personal data. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process can provide the following benefits:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the Data Protection Officer's views on the initiative.

Who is responsible for carrying out a DPIA?

The Project Manager will be responsible for ensuring that the DPIA is completed. In the absence of a Project Manager it will be the relevant specified Business Lead. The Information Governance team will assist you and explain how the DPIA should be completed.

The DPIA will require authorisation by:

- Information Asset Owner and Senior Responsible Officer
- Information Governance team or the Data Protection Officer
- Senior Information Risk Officer – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is require

Freedom of Information Act & Information Security

This document (including attachments and appendices) may be subject to an FOI request.

In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

1. Outline of the project, objectives and benefits

For transparency purposes, the DPIA and Appropriate Policy Documents reference the potential inclusion of High and certain categories of Medium risk Missing Persons. For clarification, this is a future consideration that will be subject to extended review and consultation and will not be included in Watch Lists for initial deployments of Live Facial Recognition. If pending review Missing Persons are included, all documentation will be updated to reflect this.

This DPIA will address the deployment of the Live Facial Recognition (LFR) vans by Surrey Police and Sussex Police (hereafter referenced as Sx/Sy) , it will not address the specific software used to process images, this will have its own DPIA to assess the processing and algorithms. The LFR process will also require a Super FOI to ensure all Facial Recognition data is in one place. A 'Super FOI' is an informal term used by Sussex Police and Surrey Police for reports which are likely to be of significant public interest and are proactively published in the interests of transparency and to meet our obligation under s19 of the Freedom of Information Act 2000. These reports also have the operational benefit of assisting demand management within the FOI team.

There are multiple forms of Facial Recognition Technology (FRT) that are not subject of this DPIA. This includes Retrospective Facial Recognition (RFR). RFR is also often referred to as post-event, which relates to non-real time searching of images against a database. An emerging variant of FRT is Operator Initiated Facial Recognition (OIFR) where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to proactively take an image of a particular person and then submit that particular Probe Image for analysis. Therefore, like RFR, OIFR is also out of scope for this document as it is not being used in the LFR deployments.

Live Facial Recognition (LFR) is a real-time Deployment of facial recognition technology, which compares a live camera feed(s) of faces that appear within a set zone of recognition against a predetermined Watchlist in order to locate Persons of Interest by generating an Alert to a human operator for review and consideration when a Possible Match is found.

LFR can be a valuable policing tool that helps Forces keep the public safe and to meet their statutory and common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice as well as safeguarding duties such as the location of vulnerable missing persons.

The following are illustrative examples where LFR may assist Forces to fulfil their policing duties:

- supporting the location and arrest of people wanted for criminal offences
- preventing people who are prohibited from entering an area and who may cause harm there (Watch List inclusion will be scrutinised for every deployment, as detailed in the SOP)
- 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. missing persons deemed at increased risk, etc.)

The technical operation of LFR comprises the following key stages:

- **Preparation:** Before any deployment can take place the operational process, systems, procedures and policies have to be created and compliance assured. The suite of compliance documents includes both this DPIA and the Sx/Sy LFR Legal Mandate which amongst other things outlines the considerations relevant to lawfully compiling a Watchlist including determining which persons may be on a Watchlist and the sources of Watchlist imagery.
- **Compiling/using existing database of images:** the LFR application requires a Watchlist of reference images. These are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template). The watchlist is then a collection of those biometric templates that are processed during the LFR deployment.
- **Operational pre-deployment:** The siting of the CCTV cameras, and therefore the LFR Deployment location is important to the lawful use of LFR. The LFR Policy and SOPS (Standard Operating Procedure) provide considerations relevant to the locations Sx/Sy Police may select to deploy the cameras when using them for LFR. This document only relates to Sx/Sy deployments of this technology, any other bodies or forces will be responsible for producing their own DPIA's and associated compliance.
- **Facial image acquisition:** Once the deployment begins a CCTV camera provides a live digital video feed of the 'zone of recognition'. That feed is then processed to identify within that feed pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition.
- **Face detection:** Once a CCTV camera used in a live context captures footage of a facial image, the LFR software detects individual human faces and isolates them in order to undertake further processing.
- **Feature extraction:** Taking the isolated and detected faces the software automatically extracts facial features

from the image, creating a unique Biometric Template for each face detected in the live feed.

- **Face comparison:** The LFR software then takes the contemporaneously created Live Feed biometric templates and compares each one against the list of biometric templates that comprise the Watchlist.
- **Matching:** When the biometric templates 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. The Threshold Value is detailed in the SOP and will be reviewed prior to deployment.
- **Alert and Review:** Trained members of police personnel will review all Alerts and assess the accuracy of the identification then 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 and supports compliance with the Article 8 (Human Rights Act) considerations and the right not to be subject to automated decision-making.
- **Follow up Action:** This is detailed in the SOP.
- **End of Deployment:** This is detailed in the SOP.

2. Describe the intended use of personal data:

a) Describe the nature of the processing:

Deployments will involve a real time capture of the Biometric Templates of any individuals who cross the path of the camera therefore that particular cross section of the general public will have their image and biometric template data processed (i.e. both personal data (the image) and sensitive/special category data (the biometric template).

The Watchlist will be compiled from images processed by the Police under the UK GDPR and Part 3 of the Data Protection Act depending on the purpose of each particular image being included on the watchlist. This will include, but is not limited to, custody images taken using PACE powers and retained in compliance with PACE and MoPI. All images used for deployment will meet operational thresholds clearly detailed and recorded by the officer as well as all other compliance requirements (such as to accuracy for example).

It is possible that the personal data of individuals under the age of 18 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 (or potentially where there is a law enforcement purpose to locate these persons).

Categories of data subjects in relation to the watchlist processing could therefore fall under the below categories:

- Persons suspected of having committed or being about to commit a criminal offence
- Persons subject to preventative Orders
- Persons convicted of a criminal offence
- Children or vulnerable individuals – including missing persons (subject to the parameters outlined at the start of the DPIA).

Additional information is also created in the form of metadata i.e. time, date and location. Where an individual is engaged by an officer following a Possible Match, then other details such as their name may be captured. However, all activity arising following any decision to act on a match is out of scope of the LFR activity and covered by other documentation relating to the usual exercise of police powers.

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 Templates for the watchlist are required to be deleted as soon as possible post Deployment and in any case within 24 hours.

The criteria for Watchlist constructs must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. The AO will be the rank of Superintendent or above to ensure resilience in deployment of this resource. Full guidance on this process and necessary criteria will be detailed in the SOP.

Force Authorising Officers will ensure the guidance is sufficient and covers all requirements necessary to ensure the lawful creation of the Watchlists. This guidance will be regularly reviewed to ensure compliance. As well as the detail in the SOP, training inputs will be considered by the Force Authorising Officers where requested.

Watchlists, and any images for inclusion on a Watchlist, must also be limited to the categories of image articulated LFR supporting 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; (subject to the parameters outlined at the start of the DPIA) ; and/or
e. presenting a risk of harm to themselves or others.

Images are typically imported into the LFR application for each Deployment from local Force systems. Data may also be provided by other police forces and agencies associated with law enforcement and also from the general public. Where police originated images other than custody images are considered for use, consideration regarding the legality and necessity of the inclusion of such images is needed.

Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a lawful policing objective and the proportionality of using such images on an LFR Deployment. Images, including those provided by the public, will also be assessed by reliability and accuracy.

Where it is viable to do so without unduly impacting on the performance of the LFR application, Force policy documents should provide that suitable police-originated images are preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by the Force, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.

Non-police originated images should only be included in a Watchlist with the authorisation of the AO. The AO should also consider all the circumstances pertaining to the image and in particular the factors above.

The Watchlist is created via a CSV file and corresponding Candidate Images which are saved in a secure folder with the force ICT domain. The content of the folder is extracted into the LFR application prior to Deployment via an encrypted USB drive. This device is plugged into the vans whilst on Police premises, the disk does not leave the police site. This mitigates the concerns for loss.

Force policy documents should also provide that the composition of Watchlists:

a. must be based on the intelligence case, reviewed before each Deployment to ensure that all images meet the necessity and proportionality criteria for inclusion, and the make-up of the Watchlist should not be excessive for the purpose of the LFR Deployment; and
b. must only contain images lawfully held by police with consideration also being given as to:
    - the legal basis under which the image has been acquired; and
    - the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk
    - must only use images where all reasonable steps have been taken to ensure that the image:
        - is of a person intended for inclusion on a given Watchlist; and
        - is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR application generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Images should be imported into the LFR application immediately prior to Deployment and no more than 24 hours prior to the commencement of the Deployment in order to ensure the Watchlist is current.

The addition to the Watchlist will also need to be a proportionate response to the need to manage the risk of harm. Addressing the risk of harm in this context will need to have a legal basis under a policing common law power or another legal power. 'Harm' may include a risk of harm arising in relation to a person's welfare and/or a financial harm including as a result of fraud of other dishonesty.

LFR Deployments

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 collection of personal information is via 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 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.

It has been confirmed by the business leads that both the biometric templates and the actual CCTV footage captured during the deployment will be deleted at the end of the deployment (at the latest within 24 hours of the termination of the deployment). This is a necessary process to ensure compliance with the obligations to process data fairly proportionally and for no longer than is needed as well as to encourage the support of the public when deploying this tactic.

Whilst some CCTV footage is retained for 31 days, Sussex Police and Surrey Police have considered infringements on the rights of the data subjects and more importantly, respect of their Article 8 Human Rights. Forces have therefore taken the decision not to retain the CCTV captured during an LFR deployment. This was supported by the business leads and the Data Protection Officers, who stated that deployment of LFR is not a general surveillance tool like Public Facing CCTV, it is specifically there to compare images with the watchlist.

However, there may be operational policing exceptions to this whereby the data will be retained for a longer period, these being:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996;
- in accordance with Sx / Sy Police's complaints / conduct investigation policies.

Any loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether or not protected by encryption, must be reported immediately to the Gold Command immediately and notification to the AO and DPO as soon as reasonably practicable, and where possible within 24 hours of the incident.

Not every person that is captured via the CCTV will be processed in the application. The face has to be of sufficient 'quality' to be processed into the application. The level of processing will be dependent on many factors, the significant of these include;

- crowd density,
- individual movements,
- face angle;
- lighting.

It is the intention during each deployment to allow the LFR application to process as many individuals as possible. No additional information will be attributed to the images of individuals enrolled into the LFR application.

Any Biometric Templates which do not create a Possible Match against those on the Watchlist are deleted immediately. Where there is a Possible Match this will generate an Alert which is displayed to the LFR Operator. 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.

The force will have a:

a. LFR Authorisation Process Guidance Flowchart or equivalent document which clearly sets out the decision- making steps to use LFR
b. LFR Standard Operating Procedure, or an equivalent document which should include details of:
    - factors to consider relating to the Force's use case and policing priorities for LFR
    - criteria for Watchlists and sources of imagery
    - Threshold settings
    - guidance when an Alert is generated, actions to be taken following an Alert the resourcing of Deployments to respond to Alerts and relevant officer policing powers
    - factors to consider when deciding on Deployment location and camera placement
    - arrangements to ensure the Deployment is overt, including considerations regarding any prior notification and signage
    - responsibilities of officers and staff involved in Deployment
    - retention periods

b)

c) Describe the scope of the processing

Personal data which is already accessible and processed by the police (held in source systems such as Niche RMS, provided by third parties (such as MISPER images) and other data processed by the Police for a Law Enforcement purpose) will also be processed in conjunction with the use of LFR. This may include but not limited to the name, date of birth and address of an individual. These details will not be included in the actual LFR Deployment of facial recognition technology but would be processed in the event of a Possible Match and therefore should be considered outside the scope of this DPIA. Personal data processed in respect of individuals who are to be included in the Watchlist will include name, date of birth, occurrence numbers, photograph etc which are processed for compatible purposes in any event.

With regards Sensitive and Special Category data, as the location of the deployment could identify or imply certain characteristics, the below options have been included. For example, deployment at a protest could identify a data subject's political or religious beliefs. For this reason, processing of special / sensitive category data could fall under the below (this will be discussed in more detail later in the DPIA Section 2).

- Race
- Ethnic origin
- Political opinions
- Religion
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Sexual orientation
- Health

FRT algorithms are developed to eliminate or reduce any bias involving these categories as part of the Public Equality Duty and compliance with obligations arising from the Equality Act 2010 must be demonstrable. S149 states:
'A public authority must, in the exercise of its functions, have due regard to the need to:

- eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act
- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it
- foster good relations between persons who share relevant protected characteristics and persons who do not share it.'

Typical Deployments in forces already using the technology have resulted in Watchlists of between 500 – 700 images however volumes will vary according to the necessity and proportionality for inclusion for each Deployment.

The number of individuals whose faces will be processed by the LFR cameras is unknown but is likely to be high volume. The below details the retention Particular to the LFR Application:

- **Biometric Templates – no matches**
  Any Biometric Templates which do not create a Possible Match against those on the Watchlist are deleted immediately.
- **Possible Matches**
  Where there is a Possible Match this will generate an Alert, which is displayed to the LFR Operator. If a Possible Match is made, thumbnail images will be saved within the application along with the related metadata. The first is the Candidate image, the second is the face extracted from the CCTV and the third being the CCTV frame from which the Probe Image was extracted. 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
- **Watchlists and associated metadata**
  Deleted immediately after Deployment or at latest within 24 hours. This will be detailed in the SOP.
- **LFR Operator and Engagement Logs**
  Retained in line with the MOPI retention periods. The geographical area will be determined by the purpose of the Deployment however the intention is to focus LFR overtly over a distinct geographically limited location or event which is relevant to the force area. The AO will define the **date, time, location and duration** of the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment. This is clearly recorded in the SOP and officers will be personally accountable if they do not follow this requirement.

  Whilst LFR may be used at locations across Sussex and Surrey, any Deployment will be limited to a specific location using hardwired cameras linked to the LFR application. The locations used will be based on the intelligence case to deploy LFR, the requirements of the LFR application and considerations relating to privacy that may attach to a particular area. These controls assist the public and decision-making officers to understand LFR and foresee where it may be used.

d) Describe the context of the processing:

Members of the public

- During any policing operation where LFR is deployed, signs publicising the use of the technology must be prominently placed in advance (both outside and within) the Zone of Recognition
- These measures are to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition.
- In advance of the Deployment social media and the force website may be utilised to publicise details. This will be decided on a case by case basis, considerations of which will be outlined in the SOP.
- Any member of the public who is engaged as part of an LFR Deployment should, in the normal course of events, be referred to the Sx/Sy Police Single Online Home page for more details.

Watchlists

- Those included in the watchlist will be a mix of: individuals suspected of criminality and who are wanted by the courts and police; individuals who may pose a risk to themselves and others; and individuals who may be vulnerable. Any particular deployment watchlist may comprise only one or a mix of all of these categories (where there is a mix the deployment watchlist will be a composite of several purpose specific watchlists such as say a list of persons wanted on warrant).
- There is a reasonable expectation that personal information will be processed for the fulfilment of operational police duties including:
  - Protection of life
  - Preserving order
  - Preventing the commission of offences, and
  - Bringing offenders to justice
  - Safeguarding duties.
- Where it is strictly necessary, proportionate, in pursuit of a legitimate aim and in accordance under Law Enforcement purposes.

- Children/Vulnerable Groups The LFR Operator has the ability to delete images from the Watchlist and will record such action in the operator log. This allows for potential removal of certain data, such as children.

- It is possible that there will be processing of live CCTV footage and biometric template data of children or vulnerable groups both within the watchlist and as regards those caught within the zone of recognition.
- In relation to those caught within the zone of recognition, if their Biometric Template does not generate a Possible Match no other details will be processed and the relevant information for those persons will be deleted immediately. Where there is a Possible Match, the LFR Operator will be Alerted and further manual checks will be carried out to identify whether that person is on the Watchlist. Again, if ultimately there isn't determined to be a match the relevant data for those caught within the zone of recognition will then be deleted immediately. There is no automated decision making in the process.
- Each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be aged under 18-years-old and under 13-years-old or are known to be otherwise vulnerable. Consideration must then be given as to whether any modifications are needed to the deployment in light of this or not.
- If LFR is to be used to locate a person aged under 13-years-old, specific regard should be given to anticipate LFR application performance issues. Specific advice must (at this time) be sought from Special Legal Casework and the LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO.

General Issues of concern that might potentially apply as identified by third parties (to include the public, related Commissioners and Regulators and civil libertarian groups)

- Proportionality and lawfulness – there are concerns that Deployments will 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. Also, the amount of personal data being processed is excessive and indiscriminate. Another concern is LFR may be used where it may be more appropriate to employ less intrusive methods.
- Safeguards – there are concerns that there are insufficient safeguards around the use and Deployment of LFR.
- Function creep – there are concerns that LFR will be used to monitor movements and action of the public beyond the scope of targeted Deployments or be used for covert surveillance.
- Retention – there are concerns that all data captured during a Deployment will be kept as intelligence. There are also concerns that False Alerts may result in personal data being retained for longer than necessary.
- Discretion – There have been concerns that there is too much discretion left to officers around the "who" and the "where" of Deployments.
- Bias – there are concerns that the software algorithm may contain inherent bias with regard to the protected characteristics of race, age and gender. The National Physical Laboratory: 'Facial Recognition Technology In Law Enforcement Equitability Study', referred to as the NPL Equitability Study, considers this area of further detail: frt-equitability-study_mar2023.pdf (science.police.uk)
- The human failsafe of an officer checking the image when a Possible Match is perceived as not sufficient to meet the Public Sector Equality Duty

- Legislation – it is acknowledged that there is always an opportunity to strengthen the legislative landscape for law enforcements use of emerging biometrics, but it is worth noting that this could be said of almost any area of public body activity. The National Police Chiefs Council (NPCC) are keen to continue to engage with the Home Office with regards the Department of Science, Culture, Media and Sport Data Reform Consultation.

This impact assessment will seek to address these points, eliminating or mitigating risks as far as practicable and identifying and assessing any residual risks.

e) Describe the purposes of the processing:

LFR can be a valuable policing tool that helps Forces keep the public safe and to meet their statutory and common law policing duties, which include the prevention and detection of crime, the preservation of order, the bringing offenders to justice and wider safeguarding duties. The following are illustrative examples where LFR may assist Forces achieve their policing purposes:

a. supporting the location and arrest of people wanted for criminal offences
b. preventing people who are prohibited from entering an area and who may cause harm there (e.g. 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
d. supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

For those not on the Watchlist who pass through the zone of recognition and so have their data processed by LFR there will be very minimal impact or intrusiveness. Where no alert is generated, the processing is limited to the contemporaneous CCTV feed and the creation of a biometric template from that as well as the comparison of that template against those on the watchlist. All of which happens within seconds and is contained entirely within the secure LFR system in a way that will be essentially imperceptible to the data subjects (bar the related signage and privacy notices etc). Where there is an Alert generated further processing will occur. Such alerts are internally and privately referred to an officer to compare the images. If the officer does not agree there is a match no further processing or action will take place and the CCTV footage and related biometric template will be deleted. However, if the Officer does consider there is a match in relation to the alert generated they will consider what further action is necessary and appropriate, this may include speaking with or stopping the identified individual. The signage and information around the target location, and the policies that regulate the location of deployments mean that individuals should always be able to choose not to be in the vicinity of the LFR.

It is recognised that exercising a choice not to be in a vicinity could be extra difficult when attending a protest or demonstration that may be in or go through a particular deployment location. The use of LFR can assist in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. In deciding the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of the LFR Deployment.

Article 10 and 11 rights must be weighed against the need to use LFR to enable an assembly that might otherwise be disrupted by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of LFR. If LFR is to be deployed to a protest or demonstration, the POPS Silver should define clearly why it has been adopted as a tactical option and how the deployment supports the Gold strategy. The decision should make reference to the 'Structured Approach' to balancing Article 9-11 rights against wider public concerns as set out by the College of Policing. A Bronze commander should have operational control of the equipment and its deployment. Even where a POPS command structure is in place, AO authority will be required. Consideration should be given to the specific circumstances in each case and regard should be had whether for example to balance the rights against public/demonstrator concerns in such situations it might be appropriate to give an indication publicly as to the purpose of the watchlist in such deployments. For example a person who has concerns about attending and exercising their rights to protest when LFR is deployed may not have such concerns if it is known that it is only being used to identify those who have outstanding arrest warrants for violent crimes and is not being used to collect data on normal protestors.

In an austere climate, 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. It is also the case that LFR may be the more proportionate and privacy enhancing approach compared to other methods of location and so be more proportionate as a consequence. For example, where a large number of persons are sought at a crowded location the usual method of supplying all Officers present with a paper copy of the photographs of all the wanted persons involves significantly more processing of personal data, that is inherently less secure and involves a far larger number of persons being exposed to that data than would be the case if the individuals were simply included on a watchlist in a closed and secure LFR deployment.

3. Consultation:

A number of stakeholders have been engaged from the outset of this project to ensure legitimacy and transparency in terms of privacy and its potential impact upon communities. The following have already been consulted, but the list remains organic along with the DPIA itself as Deployments mature and develop.

1. Information Commissioners Office - In 2019 the ICO commissioned a report on use of LFR for law enforcement purposes in which the following public opinions were obtained:
   - 82% of those surveyed indicated that it was acceptable for the police to use LFR;
   - 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;
   - 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime; and
   - 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.
   - The public's support holds up even if they were to be stopped by the police as a result of LFR matching them (erroneously) to a subject of interest. 58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.
2. College of Policing – with the provision of guidance on deployment and the requirements as outlined in the Authorised Professional Practice for LFR.
3. National Police Chiefs Council - assistance and guidance provided via ad hoc meetings alongside attendance at the NPCC Facial Recognition Technology Board and the NPCC Facial Recognition Working Group.
4. Office of the Police & Crime Commissioner for Surrey – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.
5. Sussex Police & Crime Commissioner - early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.
6. Both Surrey and Sussex Independent Ethics Committee – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.
7. Surrey County Council, West Sussex County Council, East Sussex County Council and all districts and boroughs - early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.
8. South Wales Police, The Metropolitan Police, Essex Police, Hampshire & Isle of Wight Constabulary Police – professional discussions around lessons learned and the creation of a LFR capability within a force.

Weightmans Review:

All documents have been reviewed by Weightmans. The recommended changes have been accepted and included in this document. However, of note is the below comment which has Data Protection Officer (DPO) agreement:

- *Will these vans be owned by one or other of the forces or are they a mutually owned asset. In other forces where I have addressed this issue the vans have been a 3rd party asset and each force was running as its own solo data controller but they in essence collaborated on documentation and just issued two copies with different force names. This way there were no joint controller or processor issues etc. I am not sure what the setup is here for Sx/Sy the use of that singular term seems to suggest the vans might be joint owned and/or you want to run this as a joint controller set up. We need to rapidly bottom this out because it will have knock on for all the documentation and compliance.*
- *If for example one force only has the trained specialists to operate the vans we need to perhaps have a processor contract in place unless we can set up a secondment/mutual aid or similar set up, alternatively we might need a joint controller arrangement.*
- *Have you bottomed out the overarching structure to the ownership and usage of the vans in terms of data responsibility, are the forces acting together or are they each acting alone using a shared resource, is there are processing done*

Both DPO agree with the above that any other Forces using the LFR hardware act as sole data controller, as such they are responsible for all governance documentation and also for any data processing. This needs to be documented in the SOP or other documentation about the shared access to the hardware.

Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair and lawful:

a) Lawful basis for the processing of personal data is stated as follows:

Personal and Special category / Sensitive data will be processed under the UK GDPR (Missing Persons) and Part 3 of the Data Protection Act for a Law Enforcement purpose. For this reason, the below list of potential processing covers all potential data processing.

- **Personal Data (Article 6 (1) of the UK GDPR):**
  (e) **Public task**: processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  (d) **Vital interests**: processing is necessary to protect someone's life.

- **Special Category Data (Article 9 (2) of the UK GDPR) to include Article 10 (Criminal Data):**
  (c) Processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
  (g) processing is necessary for reasons of **substantial public interest** (see below for the conditions), on the basis of Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The following conditions apply to this processing:
    - Administration of justice and parliamentary purposes
    - Preventing or detecting unlawful acts
    - Safeguarding of children and individuals at risk (as defined at Section 18 of Schedule 1 DPA 2018)

- **Lawful basis for processing sensitive data for law enforcement purposes:**
  Sx/Sy police will process Personal / Sensitive Data under Police's legal functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The definition of a function for 'law enforcement purposes' covers activities that are for the 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

  In addition, the police will only process sensitive data under Part 3 of the UK GDPR where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8, Part 3 Data Protection Act 2018 namely:
  - Judicial and statutory purposes/administration of justice; the sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities. In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.
  - Safeguarding of children and of individuals at risk; this condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest and is to protect them from harm or to protect their well-being.

Signs publicising the use of LFR must be prominently placed in advance (both outside and within) the Zone of Recognition. This measure is to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition (and policies relating to the location of deployments also require that there will always be an alternative route to enable such a choice).

The public must be notified in advance of the Deployment without undermining the objectives of the Deployment, details of the LFR are to be notified to the public using force websites and other appropriate communication channels (potentially including social media).

Any member of the public who is subject to an Engagement, following an Alert, as part of an LFR Deployment should, in the normal course of events, also be offered information about the technology (this will be on the Sx/Sy Police websites).

Documents will be available to the public and they will be advised of the URL for the Force website and relevant pages.

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:
LFR vans will be deployed under UK GDPR for a Public Task and/ or under Part 3 of the Data Protection Act for a Law Enforcement purpose. On deployment, a bespoke and approved Watchlist will be created and imported into the vans. Both the deployment and the Watchlist have strict conditions that they must adhere to, as such they are only deployed where necessary and no other policing tactic can deliver the necessary outcome in a more proportionate way. A key requirement in determining the deployment location and Watchlist will be considerations of the community impact and infringement of Article 8 of the Human Rights Act (amongst others).

Whilst a data subject or location may be included in a future deployment, they will not simply be 'repurposed'. All deployments are subject to the same review process, their inclusion will only be where necessary and proportionate for that specific policing purpose.

A contract will be in place with the algorithm / software supplier for the purposes of supplying the stand-alone software for the purposes of LFR deployment. The supplier does not have access to Sx/Sy Police and do not act as a data processor for the purposes of this DPIA.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:
There is a defined and documented process for the deployment of the LFR vans in Sx/Sy police. This will include considerations for any less intrusive means to achieve the policing aims. The Watchlist is generated on a case-by-case basis and inclusion of nominals will have to meet strict thresholds (including considerations of location, timings, relevance to Watchlist inclusion, etc.) before they are added. The retention of the Watchlist, biometric mapping and any images extracted will be subject to strict retention rules. For the reasons outlined in this document, all processing is considered compliant with the Principle 3 requirements.

Principle 4: Personal data must be accurate and kept up to date:
Members of the public – processing will be real time.

Watchlist – checks must be made to ensure that the images uploaded to the watchlist are the most recent and up-to-date image of the individual. Watchlists uploaded to the LFR application will not be more than 24 hours old to provide increased assurance that those on the list remain of interest.

A new Watchlist is generated for every LFR Deployment. The application assesses image quality and suitability for comparison allowing personnel to consider and manage the risk of poor quality images which are likely to generate False Alerts.

As part of the Force procurement process, due diligence must be given to expected algorithm performance (or accuracy). The National Institute of Standards & Technology (NIST) regularly undertake large scale Facial Recognition system tests. While these provide a good starting point, given algorithm-specific variation, it is incumbent upon the system owner to know their algorithm. While publicly available test data from NIST can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data sets.

There are two key metrics that determine the 'accuracy' of an LFR application and a third that details the time taken to generate an Alert. These are detailed in the below paragraphs.

- **True Recognition Rate (TRR)**. This is also referred to as the True Positive Identification Rate.
  This is the total number of times an individual(s) on a Watchlist known to have passed through the Zone of Recognition and correctly generate an Alert, as a proportion of the total number of times the individuals who pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR application or not.
  This metric can only be generated by 'seeding' known subjects (for example police officers or staff) into a **Blue Watchlist** and measuring the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated. Users of LFR applications (and vendors) must not focus so closely on maximising this metric, as it may increase the False Alert Rate to an extent that is not possible to manage the number of False alerts.
- **False Alert Rate (FAR)**. This is also referred to as False Positive Identification Rate.
  This is the number of individuals that are not on the Watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
  All of the TRR and FAR metrics should be recorded and reported to the SRO. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the number of False Alerts generated is greatly affected by the number of subjects processed by the LFR application, and to a lesser extent, the size of the Watchlist.

It should also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TRR and FAR. The Threshold needs to be set with care so as to maximise the probability of returning True Alerts, whilst keeping the number of False Alerts to acceptable levels as determined by the SRO on behalf of the force.

- **Recognition Time (RT)**. A third important metric is the Recognition Time. This is the average time taken between a subject on the Watchlist passing before a camera and the generation of an Alert. Note that the actual amount of time taken to act on an Alert will always be longer than the RT as additional time is needed for the LFR Operator to assess the Alert and to pass to an LFR Engagement Officers to then make a final decision on whether to Engage or not.
  The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

To enhance the ongoing internal understanding of algorithm and software performance, the software will be subjected to an independent academic evaluation (subject to separate DPIA) to be completed by the National Physics Laboratory. This will include an understanding equitability for age, gender and ethnic background.

The ICO has provided helpful guidance on their expectations for statistical accuracy in that it "does not mean that [the LFR] application needs to be 100% statistically accurate to comply with the accuracy principle". However, Sx/Sy Police gives due regard to the opinion that the frequency of monitoring the algorithm should be proportionate to the to the impact of an incorrect output on an individual therefore Sx/Sy Police provides for an ongoing evaluation and a post Deployment review process on a per Deployment basis.

Sx/Sy Police personnel will take all reasonable steps to ensure that each image on a Watchlist does actually pertain to the intended person. No action will be taken against an individual without human consideration of a valid match.

Any retention beyond a Deployment will be in accordance with the UK GDPR and Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or* in accordance with complaints / conduct investigation policies.

Technical systems and standard operating procedures help ensure that data is properly retained or deleted. A post-Deployment review process and associated internal audit function provides assurance in this regard.
Processing mechanisms, LFR policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes

During the Deployment there will not be any additional identifiers created or attached to the Biometric Templates of members of the public captured by LFR. Where there is no match to the Watchlist the image and biometric template will be deleted.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

- **Biometric Templates – no matches**
  Any Biometric Templates which do not match those on the Watchlist are automatically deleted immediately following the comparison process.
- **Possible Matches**
  Where there is a Possible Match, this will generate an Alert, which is displayed to the LFR Operator. If a Possible Match is made three thumbnail images will be saved within the LFR application along with the related metadata. The first is the Candidate Image from the watchlist, the second is the face extracted from the CCTV and the third being the CCTV frame from which the Probe Image was extracted. 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 finishing.
- **Watchlists and associated metadata**
  Deleted immediately after Deployment or at latest within 24 hours
- **LFR Operator and Engagement logs**
  Retained in line with MOPI retention periods.

- **CCTV Footage**
  CCTV footage generated from LFR Deployments is deleted at the end of the deployment (or within 24 hours where not possible at the end of the deployment), except where retained:
  - in accordance with the UK GDPR, Data Protection Act 2018, MoPI or the Criminal Procedures and Investigations Act 1996;
  - in accordance with Sx / Sy Police's complaints / conduct investigation policies.
- **Source System** – Niche Record Management System

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:
There are two types of access available to the application, 'user' and 'administrator' access levels. All operating staff will all be vetted and cleared to at least MV/SC level.

Role- based access controls
- Access is only granted to users following completion of training.
- The application has an in built and robust audit file log.
- Each LFR Operator will be given a username and password which they will be forced to change on initial use of the application. Local network passwords are security protected.
- The application is non-networked and non-configured to extend to the cellular network – essentially an additional geographical protection.
- As a contingency against the technology failing and requiring the LFR Operator to wipe and reset the system, the encrypted USB memory stick is retained with the LRF Operator until the end of the Deployment meaning that they are able to reimport the watchlist to the rebooted LFR application enabling the Deployment to continue.

The use of LFR technologies is governed by a number of codes of practice including those applying to the police such as PACE.

In particular the use of LFR is covered in the twelve principles laid down in the Surveillance Camera Code of Practice, to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras applies to their use by the police and other authorities.

The governance and authority for an LFR Deployment is contained in the LFR Policy. No Deployment is permitted without authorisation. The criterion for deployment is provided in the Policy. During Deployment command teams are required to monitor and review data processing to ensure that it remains lawful. A post Deployment debrief and review is used to identify lessons for the future and periodic audits will be conducted to provide assurance.

Supporting documents created include a Community Impact Assessment, an Equality Impact Assessment and an overarching Data Protection Impact Assessment (DPIA). Appropriate policy document (general and law enforcement processing) have also been created outlining the safeguards and controls in place has been created for processing under the UK GDPR and for Law Enforcement Purposes. These are public facing for transparency purposes.

The authorising Superintendent must ensure that all issues have been adequately identified, documented, and mitigated to ensure that the Deployment is not only necessary, but also proportionate to the policing purpose.
- **Operational risk assessment** - A documented assessment of specific operational risks associated with an LFR Deployment including decisions taken regarding mitigation.
- **LFR Application** – the application explains how the proposed use of LFR is based on intelligence. The application should set out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, proposed minimum agreed Threshold and rationale, and resources
- **Performance metrics** - A document detailing those metrics which will be gathered and used to assess the benefits of the operation. This may also be covered by forces in their LFR applications and/or in a force's LFR policy

- **Written Authority Document** - The AO's written authorisation provides a decision making audit trail demonstrating how the AO has considered the LFR Application and is satisfied with the accountability, legality, strict necessity and proportionality of the Deployment, the safeguards that apply to the Deployment and the alternatives that were considered but deemed to be less intrusive to realise the policing purpose. The document will detail (or, if covered in the LFR Application and/or at a Force policy level, authorise) the approach to:
  - consistently clear and appropriate signage that takes full account of predictable routes how fair processing information will be made available in public spaces where LFR is being deployed and on police websites; and
  - how individuals can exercise their rights under data protection law
  - the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR Deployment
  - The agreed minimum Threshold to be utilised during the Deployment
  - The written approval must be retained for audit purposes
- **Deployment logs** - Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Silver and Bronze Commanders, and LFR Operators and LFR Engagement Officers. These logs should include the similarity threshold set for each Deployment and any changes made to the threshold during the Deployment with a supporting rationale
- **Deployment Record -** Records details of where and when a Deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.
- **LFR Cancellation** - Records details of where and when a Deployment was carried out, the circumstances that brought a Deployment to a conclusion, what resources were used, relevant statistics, outcomes and summary of any issues following a post-Deployment review.

Following the conclusion of any Deployment the force will apply learning including evidence of effectiveness in similar operational scenarios and to carry it forward to subsequent Deployments to ensure the use of LFR on each successive occasion is truly beneficial, in particular to the public.

Watchlist images are transferred onto the LFR application via a USB using an AES-CBC 256-bit full disk hardware encryption engine that is further protected by pass number access. Access to the USB stick containing the Watchlist is limited to those with a need to use it. Full details of access (update and read only) will be detailed in the LFR Standard Operating Procedures and will be the responsibility of the business leads to ensure compliance.
Despite the encryption on the USB stick, any loss will be processed as a potential data breach using the SABR form. This follows standard Sx / Sy Police processes. However, it is important to note that the encryption and fact that the USB stick will not leave police premises will further mitigate any risks of breaches.

The data is held securely on Sx/Sy Police systems accessible to officers and staff which is fundamentally permission based. Officers leaving Sx/Sy Police automatically have their account disabled and therefore would no longer have access to the information. The data held on systems is not specific to LFR (it provides LFR with the information needed to compile and generate a Watchlist and relates to policing information generated following LFR Alerts).

Where an Alert is generated due to a Possible Match, there is an Adjudication to assess the images and where necessary engage with the individual identified as a Possible Match before any further action is taken. If during Deployment a Watchlist image generates more than one False Alert, then consideration will be given to raising the threshold for Alerts for that Watchlist subject.

The use of LFR as a tool to locate Persons of Interest will be considered alongside other policing tools and tactics. For all deployments, consideration will be given as to the effectiveness and intrusiveness of other viable methods that might produce the same result, with the least intrusive, viable method being adopted to progress an investigation.

LFR Documents provide for the training of officers and staff involved in LFR Deployments, training will be given to all officers deployed, this can verbal or in writing depending on the purpose for deployment.

7. Personal data will be processed in accordance with the individual's data protection rights:
As this will be an overt tactic and signage deployed, individuals will be able to avoid the area in which the Deployment is located. Each Deployment will have a compelling, legitimate grounds which are documented beforehand.

- Right to be informed – members of the public will be informed prior to a Deployment. Post Deployment and dependent on the passage of time it will depend on whether an individual was identified as a match as to whether this right can be exercised although individuals can be provided with the details of the time, date and location of the Deployment to determine the likelihood that their data was processed. Watchlists could be re-engineered therefore it is possible that individuals on a Watchlist may be able to exercise this right where appropriate.
- Right to rectification – individuals will be able to challenge the processing where a Possible Match has been identified by LFR and the LFR Operator/LFR Engagement Officer.
- Rights of Access – CCTV footage and the Watch List will be manually deleted at the end of the deployment (and in worst case within 24 hours), there is unlikely to be any requests for this data within this period.
- Right to erasure – a request can be submitted where a match has been made and individuals are challenging the outcome. It is acknowledged that this right is not likely to be exercised as personal information relevant to the LFR application is deleted with 24 hours.
- Right to data portability – not applicable.
- Right to object – not applicable under Part 3 DPA 2018. Sx/Sy Police will assess any right to object requests it receives on a case-by-case basis if a request is received and the processing in question does fall under Part 2 of the DPA 2018.
- Right to object to automated decision-making including processing – no automated decision making will be taking place without any human involvement. All decisions will have manual intervention.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:
Data will not routinely be processed outside of the UK.

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:
Sx/Sy Police has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of the Police to be open and transparent (wherever appropriate and possible) about how data is processed. To this end and having considered the risks to this right posed by the use of LFR, Sx/Sy Police has adopted a number of measures to ensure that the right to be informed is upheld.
A key measure is the publication of Sx/Sy Police Privacy Notices, Policies and key LFR Documents on the Sx/Sy Police website. Whilst Sx/Sy Police is not required to publish a number of these documents, it has elected to do so. This is an important measure to inform our communities including the public passing an LFR deployment and those who may be placed on a Watchlist to understand the standards Sx/Sy Police, as a public body, operates to. In this way, Sx/Sy Police use of LFR is both foreseeable and assessable. The published documents provide information as set out in the table below.
Privacy Notices:

- Data Controller identity and contact details
- Data Protection Officer details
- The scope and purposes for processing personal data
- Data retention periods
- Data sharing arrangements
- Data security
- Rights as a data subject (including access, rectification and erasure)
- Complaints (including the right to make a complaint to the ICO and contact details).

Policy Document

- An outline, strategic intent and objectives for the use of LFR and how personal data will be used by the LFR application
- Key terms used across LFR Documents
- Data retention periods applicable to LFR

LFR Legal Mandate

- The lawful basis for processing data in relation to LFR. Including in relation to:
  - Common law policing powers
  - Human Rights Act 1998
  - Equality Act 2010
  - Protection of Freedoms Act 2012
  - Data Protection Act 2018
  - UK General Data Protection Regulation
  - Freedom of Information Act 2000

LFR SOP

- Outlines measures relevant to considering when and where LFR can be Deployed.
- Watchlist considerations including the basis on which images may be added to a Watchlist and considerations relevant to the sources of non-police originated imagery.
- Provides that during any policing operation where LFR is Deployed officers will be available to assist member of the public with queries, and:
  - signs publicising the use of the technology must be prominently placed in advance (both outside and within) the Zone of Recognition; and
  - any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology.
- Both of these measures will be easy to read and together will ensure those passing the LFR technology/who are Engaged by it will have the opportunity to seek further information. Both the signs and leaflets will provide an accessible QR code and website link to the website for more information.

LFR DPIA

- Describes the nature, scope, context and purposes of the processing.
- Assesses necessity, proportionality and compliance measures.
- Identifies and assesses risk to individuals.
- Identifies any additional measures to mitigate those risks.

LFR Appropriate Policy Documents

- Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the DPA 2018.
- Explains how the processing of special category data under Part 2 Data Protection Act 2018 and Article 9 UK General Data Protection Regulation (GDRP).
- Explains how LFR processing complies with the applicable Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of sensitive or special category personal data.

4. Identifying and assessing risks

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix. The listed 'agreed actions' have been identified as a way to either reduce or eliminate risks identified as medium or high. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

Identify risk – Cause, event, effect	Likelihood	Impact	Risk	Measure to reduce or eliminate risk	Risk Treatment	Residual Risk
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.	M	M	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 Surveillance Camera Commissioner's Camera Code (as required under s29 of the Protection of Freedoms Act 2021).	Reduced	L
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.	M	M	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.	Reduced	L
Risk that the images included for a Deployment may be excessive.	M	M	M	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. 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.	Reduced	L
As a result of limited availability of images for testing the software there is a risk that bias may not be sufficiently eliminated in the algorithm deployed resulting in a disproportionate number of individuals with protected characteristics being identified in False Alerts leading to potential legal challenge, financial claims and an increase in complaints.	M	H	H	Assurances around the testing conducted by the software supplier are required in the contract and will be continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified 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 and deployment outcomes. The force will monitor performance in this regard and having ongoing obligation to consider whether other algorithms should be used instead.	Reduced	L
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.	M	H	H	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. Also, the policies and practice will ensure that the location and timing of the deployment are reasonable proportionate and justified to ensure against excessive processing.	Reduced	L

Due to the similarity in requirements for LFR 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 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.	L	H	M	Sx/Sy Police LFR Policy 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, criteria and detail around necessity, effectiveness and purpose of Deployment to ensure it is targeted; intelligence led and time limited	Reduced	L
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.	M	H	H	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	M
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.	M	H	H	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 will need to be signed off by an officer of the required authority.	Reduced	L
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.	L	H	M	The force will have in place appropriate policy documents for LFR processing under Part 2 and Part 3 of the Data Protection Act 2018	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.	H	H	H	Sx/Sy Police LFR Policy stipulates documentation and authority required for a Deployment ensuring consistency and oversight for each Deployment, in addition to the College of Policing LFR APP and SCC Codes of Practice that must be adhered to.	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	M	H	M	As part of the LFR training appropriate data protection training will be provided.	Reduced	L

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.	L	L	L	All Sx/Sy 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	L	M	M	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 Sx/Sy Police working with other police forces, law enforcement bodies and other agencies to assist Sx/Sy Police in discharging its common law policing powers. This action will not require the sharing of biometric data but may require Sx/Sy Police to share personal data, as it would for any investigation, in accordance with Sx/Sy Police routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect the LFR application and the USB used to import the data into the LFR application.	Reduced	L
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.	L	H	M	The technology has been trialled and tested by Sx/Sy Police. NEC algorithms have also been evaluated by the National Physical Laboratory (NPL), NIST and the Department of Homeland Security and Sx/Sy Police pays regard to these findings. A trained Surrey / Sussex 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. All relevant information is logged for audit purposes. Logs are kept by the Gold, Silver and LFR Operator and LFR Engagement Officer. Sx/Sy Police LFR Documents also outline points relating to the LFR application to ensure 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 Sx/Sy Police 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.	Reduced	L

6. Information Management – Comments

The processing will also take place within the requirements of the Surveillance Camera Code of Practice which has the following principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
  - *LFR is an overt tactic that is only deployed where sufficient concern or intelligence exists. There will be a required process detailed in the SOP to justify any and all deployments.*
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
  - *The Community Impact Assessment and Equality Impact Assessment will be regularly reviewed to ensure all concerns are processed and resolved. Both Forces will continue to pro-actively engage with Ethics Committees to discuss any concerns. The DPIA will be reviewed every 2 years or when any of the above consultations raise sufficient concerns.*
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
  - *All deployments will be supported by clear signage about the processing and Data Protection compliance. This will also offer links to the Police website for copies of documentation and deployment records. In certain cases (yet to be determined) the Forces will make pro-active use of Social Media to notify of planned deployment at certain Public Order / Public Safety Events. The Forces are also publishing a Super Freedom of Information to update the public on key areas of processing.*
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
  - *This DPIA clearly details how the Watch List images, biometric template and captured CCTV footage will be used and retained. This information will be externally published on the Super FoI to ensure transparency.*
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
  - *All officers involved in the operation or support of LFR deployment will be fully briefed on policies and SOP. They will receive guidance on interacting with the public if they have to interact following a potential match and what data they need to record.*
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once its purpose has been discharged.
  - *The Watch List is customised to each deployment and only retained for a period of 24 hours. This will be deleted at the end of this deployment / purpose. Any retention of images is clearly identified in this document and will ensure compliance with retention requirements, only retained as long as strictly necessary.*
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
  - *Watch Lists will only be produced for a specific deployment. There are strict restrictions outlined to the owning Department as to who creates and has access. This will be detailed in the SOP.*
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
  - *This will be detailed in the SOP and managed by the Asset Owner (yet to be agreed in each Force).*
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- The Watch List will be on encrypted USB and will only be accessible to the creator and the officer operating the LFR / making the final review decision for officer intervention. The disk will be wiped following this deployment.
  - *There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.*
- When the use of a surveillance camera system is in pursuit of a legitimate aim and a pressing need, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
  - *The use of LFR by the Police is compliant with this requirement. Deployment will primarily be under Part 3 of the Data Protection Act 2018 for a Law Enforcement Purpose. However, Missing Persons may also be added to the Watch List where there is sufficient safeguarding concern, this is processing under Part 2 of the UK GDPR.*

- Any information used to support a surveillance camera system which matches against a reference database for matching purposes should be accurate and kept up to date.
    - *All documentation and FoI publications will be regularly reviewed to ensure they are current and address any risks or concerns from the public identified through deployment. Also, the ethical concerns of LFR will be monitored and if required, documentation updated to mitigate any potential concerns. This will the primary function of the Super FOI to ensure transparency and build community trust for this tactic.*

The above requirements form the foundation of LFR within Sussex and Surrey. The Forces are aware of the need to transparency in all processing and also the necessity for risk based deployment as opposed to overuse of the technology for the sake of it. Data Protection and Ethical concerns have been at the forefront of all discussions in relation to facial recognition tactics, especially LFR.

Business leads are aware that supporting documentation and guidance (internal and external) requires constant review and amendments to support the changing landscape and perception of facial recognition in today's society. This has also been accepted and will be supported by the business leads for each Force with support from Information Governance teams.

Challenges were made regarding the retention of the CCTV footage for a period of 31 days. This was reviewed with consideration of the rights to privacy of the data subject and impact on their human rights. The decision, as detailed below, confirms that this data will not be retained by Sussex Police or Surrey Police:

- *My rationale around it is, the CCTV in the vans is only there as a means of getting a base for the watchlist to be tested against, it is not being used in the traditional sense of CCTV. I would be supportive of it being deleted at the end of the operation. I think is relevant we would most likely be deploying this in town centres that will be highly likely to be covered by CCTV, so there is no need for this to be added into that mix and I think the tradition town centre CCTV should cover the PSD need (but I will seek their view). It might be something we can reference in the policy that the vans if practical operationally should be used in areas covered by CCTV. I would also say that the engagement with the public is also going to be recorded on BWV so that should satisfy the recording of any interaction.*

7. Authorisation of DPIA:

DPIA will be retained by the Information Governance team. This will be reviewed by the parties listed below with consideration then given for signatory by the Senior Information Risk Owner (SIRO), Senior Responsible Officer (SRO) and Information Commissioners Office (ICO) if required.

	Name	Date
Force Lead	[redacted]	*29/05/2025*
Force Lead	[redacted]	*28/03/2025*
Project Lead	[redacted]	*28/03/2025* *Review 01/07/2025*
Information Management Sussex	[redacted]	*28/03/2025* *Review 01/07/2025*
Data Protection Officer Sussex	[redacted]	*27/05/2025* *Review 11/07/2025*
Summary of DPO advice:	*The development of this DPIA has been iterative and I have been sighted on two drafts before submitting this review.* *There is legitimate public and regulatory concern about the operational deployment of this technology. Conversely however, it presents real opportunities in terms of the effectiveness and efficiency the public expects from the police service. Therefore, the use of this technology is lawful and legitimate provided it is subject to appropriate checks and balances.* *I am satisfied that the project team have engaged extremely well with the Forces' IM teams and DPOs and that privacy concerns have been addressed effectively. In part, this has been achieved by consulting other Forces on 'lessons learned'.* *I have asked for some additional clarity on the justification of using LFR to locate witnesses who are under no obligation to identify themselves to police or to co- operate with investigations. I have also sought further clarity on the level of risk at which LFR will be considered for Missing Persons inquiries (high risk or the higher threshold of threat to life).* *Update: Witnesses will no longer be added to Watch Lists. An appropriate policy stance has been adopted for Missing Persons but these will not be part of the first tranche of deployments.* *I am satisfied that the obligations set by the Data Protections Principles have been well addressed. The risk assessment is comprehensive and any high threat issued have been satisfactorily eliminated or mitigated. There has been discussion regarding the retention periods for products generated through this process and I am satisfied that the minimum practical period has now been adopted in each case.* *Whilst the technology-led aspects of the process are well set out, I have asked for additional clarity on the protection of data held on hard copy media including the USB drives proposed for deployment.* *I am pleased to note the extent to which the DPIA recognises that privacy issues will vary by type of deploy and are comparative and not absolute. In particular, the impact on the rights conferred under Articles 9-11 ECHR as regards using LFR during protest is well set out and mitigated through command and control protocols.* *Once the residual issues noted above are addressed/ clarified, I am satisfied this can be progressed with a high degree of assurance.*	
Data Protection Officer Surrey	[redacted]	*22/05/2025* *Review 01/07/2025*
Summary of DPO advice:	*I would suggest whilst this process and technology is being used initially the process/data/documents are cross referenced with this DPIA to ensure what is being advised within this document is happening with each deployment and that the documents advised that will be created are being created and adhered to. I would also suggest initially that the document suite as a whole is audited every 3 months to ensure that all documents are correct and the DPIA is accurate.*	

Referral to the SIRO (if required)

Senior Information Risk Owner	[redacted]	*14th July 2025*
SIRO Comments	As the DPO has stated regular proactive review of the process and practice will be needed. I would particularly recommend that we ensure Watchlists are bespoke for each deployment and that all officers are appropriately trained before any use of LFR.	

Referral to the ICO (if required)

Refer Name	Date	ICO Comments

DPIA Review History

Date	IGO - Force	Comments

Addendum –Public Order / Public Safety Events

As part of the ongoing LFR work, Forces are looking at deploying it to specific events with interactions remaining in Police control. Forces deploy to crime hotspots, typically town centres, but the proposal is to start deploying to events where there is the need / justification. This has been discussed with, and approved by, Chief Officers. Force Information Management Teams have been updated as it will have implications on what is currently documented in the DPIA, and some amendments will be needed.

Governance Supervisor position is that the current documents (DPIA, Policy, SOP, etc) are all over-arching governance assurances that Forces are processing lawfully. They cover the processing and retention of watchlists etc but just don't state Forces share with other law enforcement agencies for specific deployments. Following review of both Forces websites a covering statement is appropriate, and two changes as below can be applied:

The DPIA already states that deployment can be to Public Order / Public Safety Events and it is suitable that this covers this processing as long as the engagement with the public is managed by Police and is for a law enforcement purpose. However, it will be necessary to add the below text to the current Force Internet sites to ensure full transparency with this and the watchlist sharing processes, as there is a necessity to share with other Forces for similar reasons. Separate documentation about sharing has been created and will be agreed with external Forces prior to any actual processing. Public Order / Public Safety Events are defined as the use of LFR at a public order public safety events will be considered in the context of the overall operation, and LFR is one of the tactics available to commanders depending on the threat, risk and harm identified.

Annex B – LFR Terminology

The following terms and definitions apply in relation to Live Facial Recognition:-

Adjudication

A human assessment of an alert generated by the Live Facial Recognition (LFR) application by an LFR engagement officer (supported, as needed by the LFR operator) to decide whether to engage further with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject, system and environmental factors.

Administrator

A specially trained person who has access rights to the LFR application in order to optimise and maintain its operational capability.

Alerts

An alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the watchlist and returns a comparison score above the Threshold.

True Alert

A true alert is determined when the probe image is the same as the candidate image in the watchlist.

Confirmed True Alert

Following engagement, a confirmed true alert is determined when the engaged individual is the same as the person in the candidate image in the watchlist.

True Recognition Rate

It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated).

This is also referred to as the true positive identification rate.

False Alert

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement.

(The false alert rate is one of the two measures relevant to determining application accuracy).

Confirmed False Alert

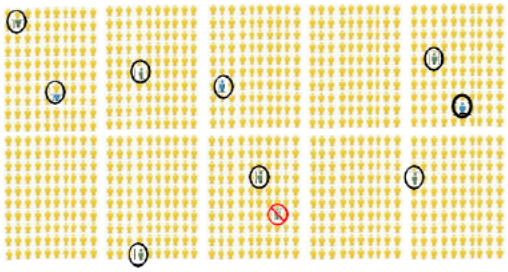
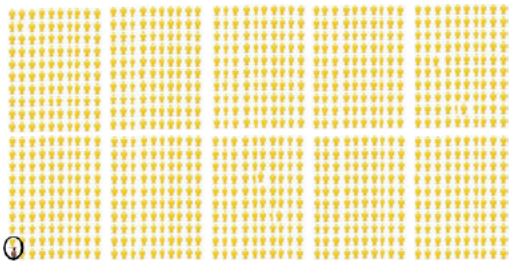
Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

False Alert Rate

The number of individuals that are not on the watchlist who generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition. This is also referred to as false positive identification rate.

Application Accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the True Recognition Rate and the False Alert Rate. This is further explained below. The example given has been simplified to demonstrate the concept, but note that the metrics have been calculated in accordance with the agreed scientific method as set out by the International Organisation for Standardisation:

		True Recognition Rate	False Alert Rate
What is it?		It is the total number of times an individual(s) on a watchlist known to have passed through the Zone of Recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the Zone of Recognition. This is regardless of whether an alert is generated by the LFR application or not.	Is the number of individuals that are not on the watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
Worked Example		 The True Recognition Rate would be 90% if 10 people on the watchlist each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people (with no alert being generated against the 10th person).	The False Alert Rate would be 0.1%, if for every 1,000 people that passed the LFR system, an Alert was generated against one person who was not on the watchlist. 

Authorising Officer (AO)
The Authorising officer (usually holds the rank of Superintendent or above) who provides the authority for LFR to be used.

Biometric Template
A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

Blue Watchlist
A watchlist comprises known persons that can be used to test system performance, for example, police officers / staff may be placed on a blue watchlist and `seeded' into the crowd who walk through the zone of recognition during a Deployment.

Candidate Image
Image of a person from the watchlist returned as a result of an alert.

Deployment
Use of an LFR application as authorised, as authorised by an AO to locate those on an LFR watchlist.

Deployment record
An amalgam of the LFR application, the written authority document and the LFR cancellation report. This sets out the details of a proposed Deployment including – but not limited to:

e. location
f. dates and times
g. Deployment and watchlist rationale
h. legal basis
i. necessity
j. proportionality
k. safeguards
l. watchlist composition
m. authorising officer
n. resources
o. relevant statistics
p. outcomes
q. summary of any issues

Engagement
An officer communicating with a member of the public as a result of an alert.

Environmental Factors
An external element that affects LFR application performance, such as dim lighting, glare, rain, mist.

Faces per frame
A configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.

Facial Recognition Technology (FRT)
This technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database and generates possible matches. This is based on digital images (either still or from live camera feeds).

False Negative
Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are a number of reasons false negatives occur; these include application, subject and environmental factors, and how high the Threshold is set.

Gold Commander
Is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment. (They are responsible and accountable for the policing operation/event and determine the strategic objectives).

Live Facial Recognition (LFR)
LFR is a real-time Deployment of facial recognition technology, 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.

LFR Engagement Officer
An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR Deployment.

LFR Operator
An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

LFR System Engineer
A person who deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of LFR system.

Person(s) of Interest
A person on a watchlist

Possible Match
A person returned as a result of the probe and candidate image

Probe Image
A facial image which is searched against a watchlist.

Recognition Time
The average time from when a face appears in the zone of recognition of the camera to when the LFR application generates an alert.

Retrospective Facial Recognition (RFR)
A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.

Silver Commander
The officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander. (The silver commander develops, commands and coordinates the overall tactical response of an operation, in accordance with the strategic objectives set by the gold commander).

Similarity Score
Is a numerical value indicating the extent of similarity between the probe and candidate image, with a higher score indicating greater points of similarity.

Subject Factor
A factor linked to the individual, for example, demographic factors or physical features or behaviours for example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.

System Factor
A factor relating to the LFR application such as the algorithm.

Threshold
The configurable point at which two images being compared will result in an alert. The Threshold needs to be set with care to maximise the probability of returning true alerts whilst keeping the false alert rate to an acceptable level.

Urgency
In the context of authorising an LFR Deployment, a Deployment that is related to an:
Imminent threat-to-life or serious harm situation; and/or intelligence / investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action.

Watchlist
A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (from the reference image database) and will have been created specifically for the LFR Deployment.

Zone of Recognition
A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.