Merseyside Police

Data Protection Impact Assessment: Live Facial Recognition (LFR)

OFFICIAL

Publication Scheme	**Government Security Classification Scheme (GSCS):** **Official.** ***The level of security classification indicates the sensitivity of information. The Policy Author will determine the classification of either OFFICIAL or OFFICIAL- SENSITIVE. A handling rule may also be added for example OFFICIAL-SENSITIVE-For Police Eyes Only.*** **Data Protection Impact Assessment on External Force Website?** **Yes – Data Protection Impact Assessment**
Department of Origin	***Matrix Force Operations***
Policy Holder	***Chief Supt Zoe Thornton***
Policy Author	***Sgt Chris Hilton***
Data Protection Officer	***Ian Boyham***
Related Information **(Insert hyperlinks to related information)**	
This Version	**1**

Date Created / Modified	11/12/2025
Review By *(3 years)*	19/03/2027

Purpose

Live Facial Recognition (LFR) is a policing tool designed to support Merseyside Police in fulfilling its statutory duties under common law and the Police and Criminal Evidence Act 1984, including the prevention and detection of crime, the protection of life and property, and the maintenance of public order.

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.

These may include persons wanted by the courts, suspects in ongoing investigations, individuals subject to bail conditions or court orders, missing persons deemed at increased risk, or those presenting a risk of harm to themselves or others.

The purpose of deploying LFR is to:

• Assist in the location and apprehension of individuals wanted for criminal offences.

• Prevent individuals who may pose a threat to public safety from entering designated areas.

• Support safeguarding efforts for vulnerable individuals.

• Enhance operational efficiency in high-football environments where traditional policing methods may be less effective.

• Reduce reliance on more intrusive tactics such as stop and search by enabling targeted engagement based on biometric alerts.

Each deployment will be intelligence-led, proportionate, and subject to prior authorisation. The technology will not operate autonomously; all alerts will be reviewed by trained police personnel before any engagement occurs. The use of LFR will be governed by strict data protection, ethical, and operational controls to ensure compliance with the Data Protection Act 2018, UK GDPR, and the Surveillance Camera Code of Practice.

Step 1: Screening Checklist

Not every project will require a full DPIA. Saying 'Yes' to questions 1-12 indicate that a DPIA is mandatory as these will be the types of intended processing that made a DPIA a requirement. Saying 'Yes' to questions 13 onwards indicate that a DPIA should be considered.

1.01 Will this process use systematic and extensive profiling or automated decision making to make significant decisions about people?

Yes

1.02 Will this process special category data or criminal offence data on a large scale?

Yes

1.03 Will this process systematically monitors a publicly accessible place on a large scale?

Yes

1.04 Will this process use new technologies?

Yes

1.05 Will this process use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity, or benefit?

Yes

1.06 Will this process conduct profiling on a large scale?

Yes

1.07 Will this process biometric or genetic data?

Yes

1.08 Will this process combine, compare, or match data from multiple sources?

Yes

1.09 Will this process personal data without providing a privacy notice directly to the individual?

Yes

1.10 Will this process personal data in a way which involves tracking individuals' online or offline location or behaviour?

No

1.11 Will this process children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them?

Yes

1.12 Will this process personal data which could result in a risk of physical harm in the event of a security breach?

Yes

1.13 Is personal data transferred to any countries outside the UK?

No

1.14 Will this process involve evaluation or scoring?

No

1.15 Will this process involve Automated decision-making with significant effects?

Yes

1.16 Is Systematic monitoring used?

No

1.17 Does this involve processing of sensitive data or data of a highly personal nature?

Yes

1.18 Will this involve processing on a large scale?

Yes

1.19 Will this involve processing of data concerning vulnerable data subjects?

Yes

1.20 Does this process use innovative technological or organisational solutions?

Yes

1.21 Does this processing involve preventing data subjects from exercising a right or using a service or contract?

Yes

DPIA Required.

Step 2: Describe the processing

2.01 How will you collect the data?
Compiling/using existing database of images: the LFR application requires a Watchlist of reference images against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template).

The LFR Policy outlines considerations relevant to lawfully compiling a Watchlist including determining which persons may be on a Watchlist and the sources of Watchlist imagery.

Facial image acquisition: a CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition and using it as a live feed. The positioning of the CCTV cameras, and therefore the LFR Deployment location is important to the lawful use of LFR. The LFR Policy and SOPS provide considerations relevant to the locations Merseyside Police may select to deploy the cameras when using them for LFR.

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

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

Face comparison: The LFR software compares the Biometric Template with those held on the

Watchlist.

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

Out of scope - There are other forms of facial recognition technology (FRT) that are not subject of this guidance. 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 submit a particular Probe Image for analysis and is also out of scope for this guidance.

2.02 How will you use the data?

The data will be used for law enforcement purposes, to identify and apprehend those wanted for offences or of interest to the police. The data will be used to compare against known individuals.

2.03 How will the data be stored?
The data (watchlist) will be stored on an encrypted USB device. The captured data from the cameras will be briefly stored electronically on an encrypted and isolated computer, before deletion in all cases, within 24 hours.

2.04 Will you be sharing data with anyone?
No

2.05 What is the source(s) of the data?
Compilation of images is taken from the Corvus system, from data contained within Niche. Facial Image Acquisition for comparison against that compilation of images is taken from live cameras.

Source System – Niche Record Management System. Please refer to Home Office Review of the Use and Retention on of Custody Images published February 2017 (recommendation 4)

Non-conviction – upon requesting.

a) Group 1 or 2 (Public Protection Markers & sexual, violent or other serious offences respectively) 10 years upon request then review.
b) Group 3 (all other offences) – 6 years upon request then review.
c) Group 4 (missing persons) – 6 years then review

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

a) Group 1 -subject is 100 years the review
b) Group 2 – 10 year clear period then review
c) Group 3 – 6 year clear period
d) Group 4 (missing persons) – 6 years then review

2.06 Attach a data flow diagram or another way of describing data flows.
The technical operation of LFR comprises the following six stages:

1. Compiling/using an existing database of images. LFR requires a database of existing facial images (referred to in this case as a Watchlist) against which to compare facial images and the biometrics contained in them. For such images to be used for LFR, they are processed so that the "facial features" associated with their subjects are extracted and expressed as numerical values.
2. Facial image acquisition. A CCTV camera takes digital pictures of facial images in real time. This case is concerned with the situation where a moving image is captured when a person passes into the camera's field of view, using a live feed.
3. Face detection. Once a CCTV camera used in a live context captures footage, the (a) detects human faces and then(b) isolates individual faces.
4. Feature extraction. Taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face, the resulting biometric Template being unique to that image.
5. Face comparison. The FRT software compares the extracted facial features with those contained in the facial images held on the Watchlist.
6. Matching. When facial features from two images are compared, the FRT software generates a Similarity Score. A Threshold value is fixed to determine when the software will indicate that a Possible Match has occurred. Fixing this value too low or too high can, respectively, create risks of a high False Alert Rate (i.e. the percentage of incorrect matches identified by the software) or a high False Negative rate.

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 other details such as their name may be captured however this is out of scope of the LFR activity.

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

The Candidate Images and related biometric Template are deleted immediately post Deployment and in any case within 24 hours.

The criteria for constructs of Watchlists for use with LFR must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. Watchlists,

and any images for inclusion on a Watchlist, must also be limited to the categories of image articulated in Force policy documents which are images of people who are:

1. Wanted by the courts; and/or
2. 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
3. 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
4. Missing persons deemed increased risk; and/or
5. Presenting a risk of harm to themselves or others.

Images are typically imported in to the LFR application for each Deployment from NICHE RMS (via Corvus) and the Police national Computer (PNC). 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 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 policing objective and the proportionality of using such images on an LFR Deployment.

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 should be 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.

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

1. 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
2. Must only contain images lawfully held by police with consideration also being given as to:
   a) the legal basis under which the image has been acquired; and

b) 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,
c) 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.

Interpretation of Watchlist categories

'Further police action required.' This term will reflect the nature of the criminal investigation underway. Where it is lawful and necessary to do so, it may include the need to arrest the individual for further policing enquiries. On other occasions, the investigation may, for example, require details to be verified with an individual to progress the investigation. Proposed further police action will be specified and recorded in advance of the decision to include an image on a Watchlist and the action proposed will be in accordance with lawful police powers.

'Missing persons deemed increased risk.' This term will be subject to the College of Policing definition of medium risk (or above) contained in Missing Persons APP. That is the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public.

'Presenting a risk of harm.' This term will be informed by the intelligence case. This will need inform the AO as to how the individual presents a risk of harm and how:

1. Using LFR to facilitate their location is necessary to manage the risk of harm identified; and
2. Why it is necessary for the police to take action in order to manage the risk of harm
   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 two CCTV cameras connected to the standalone laptop/server. The laptop is not connected to the force ICT infrastructure and can be considered a 'black box' solution (an independent system to the current technical Merseyside Police 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.

The CCTV feed will itself be saved. This processing is out of scope if this DPIA.

Not every person that is captured via the CCTV will be enrolled into the application. The face has to be of sufficient 'quality' to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include,

a) crowd density,
b) individual movements,
c) face angle; and
d) lighting.

It is the intention during each Deployment to allow the LFR application to enrol and therefore process as many individuals as possible, however it is worthy of note that processing that does not lead to an Alert will be momentary, and the image permanently deleted. No additional information will be attributed to the images of individuals enrolled into the LFR application. The application has a built-in audit trail functionality that ensures Probe Images that do not generate a Possible Match against a Candidate Image are not retained within it. The Watchlist is created via a CSV file which is saved in a secure folder along with the corresponding Candidate Images within the force ICT domain. The content of the folder is extracted into the LFR application prior to Deployment via an encrypted USB drive.

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.

2.07 What is the nature of the data?
Race, Ethnic Origin, biometric data are those categories of data may be processed which in turn may indicate an individual's age, gender and ethnic origin. FRT algorithms will be 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:

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

2.08 Does it include special category or criminal offence data?
Yes, Special Category Data and Criminal Offence Data

2.09 How much data will you be collecting and using?

a) Persons suspected of having committed or being about to commit a criminal offence.
b) Persons convicted of a criminal offence
c) Persons who are or may be victims of a criminal offences
d) Children or vulnerable individuals
e) Police officers or staff (current and former)
f) Other If other, then please provide further details below:

Deployments will be a real time capture of the biometric Templates of any individuals who cross the path of the camera therefore a cross section of the general public including all categories will potentially be processed. The Watchlist will be compiled from lawfully held images based on the criteria for the Deployment. It is possible that the personal data of individuals aged under 18 years, those under 13 years, a person with a disability or vulnerable adults will be processed where there is a policing need, and it is deemed to be necessary and proportionate to locate and/or safeguard these individuals.

The number of individuals whose faces will be processed by the LFR cameras is unknown but is likely to be high volume.

2.10 How often?
Couple or Several Times

2.11 How long will you keep it?
An Hour to a 24hours.

2.12 How will the data be deleted / destroyed?
Automatic deletion and manual corroboration.

2.13 How many individuals are affected?
1000000+

2.14 What geographical area does it cover?
Merseyside

2.15 What is the current state of technology in this area?
Available

2.16 Which categories of data subjects will this process involve?
Accused, Adult, Child, Defendant, Convicted, Suspect, Young person

2.17 Do they include children or other vulnerable groups?
Yes -Children and Other Vulnerable Groups

2.18 Will this process involve Artificial Intelligence (AI)?
No

Step 3: Consultation and Stakeholder Engagement

3.01 Describe when and how you will seek individuals' views or justify why it is not appropriate to do so.

Internal Consultation

a) Agreeing Ownership of LFR Deployment MOU.
b) Developing process for compilation of index.
c) Seek consultative feedback from the Police Federation, Superintendents' Association, Staff Associations, Unions and Support Networks.
d) Seek consultative feedback from operational Commanders (OFC, TFC, SFC, Bronze, Silver and Gold POPS).
e) Seek a bespoke Merseyside Police legal opinion from Legal Services (mandate).
f) Develop a Benefit Realisation Assessment.
g) Agree the use of terminology – Index &/or register to replace watchlist &/or database.

External Consultation – Community - Engage, Explore, Explain, Elaborate and Evaluate.

a) Engage – seek opportunities to engage; Community Advisory Groups, MIAG, Online Community Forum Session, Leaflets/posters for GEO with QR Code for feedback.
b) Explore & Explain – develop a briefing package that explains why, how and what.
c) Elaborate – develop a briefing package that sets out the legitimacy testing and results.
d) Evaluate – capture, codify and share the results of community feedback as part of the policy drafting process.

External Consultation – Political and Interest Groups - Engage, Explore, Explain, Elaborate and Evaluate.

a) Engage – seek engagement opportunities with local political representatives; Police and Crime Commissioner, Merseyside MPs, Community Safety Partnerships & Local Authority Chief Executives, PRAP Stakeholders.
b) Explore & Explain – develop a briefing package that explains why, how and what.
c) Elaborate – develop a briefing package that sets out the legitimacy testing and results.
d) Evaluate – capture, codify and share the results of community feedback as part of the policy drafting process.

3.02 Who else do you need to involve within your organisation?

a) ICT -Digital Futures
b) All Strands

c) Legal Services
d) Community Engagement
e) Inclusion Team
f) Fairness in Policing Team
g) News and Comms

3.03 Do you plan to consult, or have you consulted information security experts, or any other experts or external partners?
The Digital Futures Team have been, and are actively involved, in Merseyside Police's uptake of facial Recognition technology. The manager, Tony Jackson, is working on the introduction of LFR for Merseyside Police. At this stage there is no requirement to consult ICT security experts as Merseyside Police does not have a technological solution or LFR assets under its control. LFR deployment in Merseyside would be undertaken by external forces on mutual aid.

As part of the process the Home Office FR Policy Lead has been consulted. additional consultation has taken place with:

a) Police and Crime Commissioner,
b) Deputy PCC, Chief Officers,
c) Heads of Strand,
d) Community Safety Partnerships in Wirral, Sefton, Knowsley, Liverpool and St Helens.
e) CEOs of Local Authority.
f) MPs have been written to, explaining the approach.
g) Merseyside Independent Advisory Group, Community Advisory Groups and Police Race action Plan Stakeholders have been consulted and briefed.

An EIA and CIA have been drafted.

3.04 Are there any current issues of public concern that you should factor in?
Yes

3.05 Could you please outline the specific issues of public concern that you believe to be relevant?
Civil Liberties – Civil Liberties groups have expressed concerns regarding the use of biometric facial matching within law enforcement practices. While some of these concerns have been addressed, the organisation needs to remain mindful of the concern.

Misuse – the public are likely to have concerns that LFR will be used to (overtly or covertly) monitor the public without justification.

Retention – the public could be concerned that the police will retain images taken as part of the LFR process for other uses.

Public Trust and Confidence in policing is low nationally and whilst improving locally, deployments need to be cognisant on the impact on public trust and confidence. Public perception of invasion of privacy Facial Recognition is still a fairly new technology with advances still taking place.

Step 4: Necessity and Proportionality

4.01 Does the processing achieve your purpose?
Yes

4.02 What are the benefits of the processing for you, and more broadly?
LFR can be a valuable policing tool that helps Forces keep the public safe and to meet their common law policing dues, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

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

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

4.03 What is the intended effect on individuals?

For those not on the Watchlist who are in an area where LFR is deployed there will be no impact or intrusiveness except where there is an Alert, whereby an officer will compare the images and if necessary, can speak with the identified individual. This means that there may be a reduction in stop and search. The signage and information around the target location means that individuals can choose not to be in the vicinity of the LFR. It is recognised that exercising a choice not to be in a vicinity would be extra difficult when attending a protest or demonstration. The use of LFR can assist Merseyside Police 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.

4.04 How will you ensure data quality?
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 Merseyside Police LFR application will not be more than 24 hours old to provide increased assurance that those on the list remain of interest to Merseyside Police. Technical measures are also in place to cross reference data to the PNC to verify that individuals are still of interest prior to the

encrypted transfer to the LFR application. A new Watchlist is generated for every LFR Deployment. The application assesses image quality and suitability for comparison allowing Merseyside Police 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 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 me 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 be 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 me taken between a subject on the Watchlist passing before a camera and the generation of an Alert. Note that the actual amount of me taken to act on an Alert will always be longer than the RT as additional me 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 Police forces have commissioned 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 evaluation has assisted in measuring overall accuracy along with accuracy variations across demographic cohorts.
Accuracy will also be measured on an ongoing basis with the inclusion of Blue Watchlists. Currently this utilises the M40 algorithm supplied by NEC, this is utilised with NEC's Neoface software.

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, Merseyside 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 Merseyside Police provides for an ongoing evaluation and a post Deployment review process on a per Deployment basis.

The supplier has also been held in high regard by the NIST in its 2018 evaluation of over 200 algorithms.

Merseyside 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.

4.05 How will you ensure data minimisation?
Deployment of LFR will only be done on an intelligence, threat assessed and authorised basis.

4.06 How will you prevent 'function creep'?
Force Policy sets out specific criteria for deployment, including authority levels and deployment criteria.

4**.07 What is the nature of your relationship with the individuals (data subjects)?**
Competent Authority

4.08 Would they expect you to use their data in this way?
Yes

4.09 Does a duty of confidentiality exist?
Yes -it is in the public interest to override

4.10 Will it impact Article 8 of the Human Rights Act?
Yes -can interfere to prevent disorder or crime
Yes -can interfere for public safety reasons

4.11 What information will you give individuals?
A communications strategy will be in place for each deployment. 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.

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 (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. Any person who requires further information relating to LFR should be provided with contact information for the LFR operation.

4.12 How will you help to support their rights?
Where possible and appropriate. Individuals will be able to avoid the area in which the Deployment is located.

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.

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. Merseyside 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.
Each Deployment will have a compelling, legitimate grounds which are documented beforehand.

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.

4.13 What is your lawful basis for processing?

For general processing, what is the Lawful Condition
6.1 (e) Public task (a) the administration of justice
6.1 (e) Public task (c) the exercise of a function conferred on a person by an enactment or rule of law.

For general processing of special category data, what is the Lawful Condition.
9.2 (g) Substantial public interest/rule of law.

For general processing, what is Lawful Condition for processing Special categories of personal data and criminal convictions.
6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
10. Preventing or detecting unlawful acts
11. Protecting the public against dishonesty
12. Regulatory requirements relating to unlawful acts and dishonesty
15. Suspicion of terrorist financing or money laundering
18. Safeguarding of children and individuals at risk

For Law Enforcement processing, what is the law enforcement purpose?

a) Prevention of criminal offences
b) Investigation of criminal offences
c) Detection of criminal offences
d) Prosecution of criminal offences
e) Execution of criminal penalties

Safeguarding against and prevention of threats to public safety for Law Enforcement processing, what is the lawful condition?
The process sing is necessary for the performance of a task carried out by a competent authority (Merseyside Police is a competent authority)

For Law Enforcement processing of special category personal data, what is the lawful condition
processing?
The processing of the special category personal data is strictly necessary for the law enforcement purpose.

For Law Enforcement processing, what is the lawful condition for sensitive processing?

1. The administration of justice
2. To protect the vital interests of the data subject or of another individual.
3. To protect an individual from neglect or physical, mental or emotional harm, or protect the physical, mental or emotional well-being of an individual...

Step 5: Security Arrangements

If necessary, liaise with ICT staff about this section especially if there is an IT Project Manager. This will be mutually beneficial because it could avoid a duplication of effort by the person(s) completing this assessment and the IT personnel. This is particularly the case if data is to be subject to 'Cloud' storage because IT may have already assessed this against the 16 Cloud principles and can provide more comprehensive information for this assessment.

5.01 What are the Government Security Classifications for the data?

Official – Sensitive

5.02 Where will the data be stored?

On Premise

5.03 What safeguards are in place to protect the data?

Two types of access will be available to the application – 'user' and 'administrator' access levels.

Operating staff will all be vetted and cleared to at least MV/SC level.

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 CSV file (hashed).

Each LFR Operator will be given a username and password which they will be forced to change on initial use of the application ('Active Directory' strength of eight characters to include upper and lower case as well as being alpha numeric. 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.

The application is non-networked and non-configured to extend to the cellular network – essentially an additional geographical protection.

The LFR application is 'closed' and not connected to other Merseyside Police systems or the internet.

As a contingency against the technology failing and requiring the LFR Operator to wipe and reset it the encrypted USB memory stick is retained with the LRF Operator under 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.

Authority – the governance and authority for an LFR Deployment is contained in the MP LFR Policy. No Deployment is permitted without authorisation. During Deployment command teams are required to monitor and review data processing ensuring that it remains lawful. A post Deployment debrief, and review is used to identify lessons for the future and periodic audit provide assurance.

Merseyside Police ICT Technical Standards

Merseyside Police ICT Security Standards

Merseyside ICT polices & procedures

Merseyside ICT processes for maintenance of equipment.

5.04 Is there an external data processor involved?
No

5.07 By which method(s) do you intend to share the data with third parties? (if sharing)
N/A

5.08 What standards of security are met?
Merseyside Police ICT Baseline

5.09 Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
No.

Step 6: Informaon Risks

Information Risk 01 - Accessibility

IR01 (Read only)

The Information within Live Facial Recognition (LFR) is accessible by people who should not have access to it

IR01 Likelihood 3 Unlikely - Below 1 in 3 or 35%

IR01 Severity 3 Medium - The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR01 Risk Treatment - The images which are extracted from force systems are stored, whilst in transit, on an encrypted USB device. Occasionally, we will look to invite observes to view our operations to demonstrate the legitimacy of this process. This is to ensure transparency and mitigate any public fears. These people will be local elected officials or other known partners.

IR01 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR01 Current Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR01 Current Risk (Read only) 3

Information Risk 02 - Security

IR02 (Read only)

The Information within Live Facial Recognition (LFR) is on a system which is hosted/held on an

insecure infrastructure/environment or premises

IR02 Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR02 Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR02 Risk Treatment The images which are extracted from force systems are stored, whilst in transit, on an encrypted USB device. Occasionally, we will look to invite observes to view our operations to demonstrate the legitimacy of this process. This is to ensure transparency and mitigate any public fears. These people will be local elected officials or other known partners.

Additionally, the computer running the LFR will be air gapped from other force systems and will be secure.

IR02 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR02 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR02 Current Risk (Read only) 2

Information Risk 03 - Inappropriate Access

IR03 (Read only)

People who should have access to the Information within Live Facial Recognition (LFR) have

inappropriate levels of access to it.

IR03 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR03 Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR03 Risk Treatment Very Unlikely given the reduce cohort of users.

IR03 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR03 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR03 Current Risk (Read only) 2

Information Risk 04 - Inappropriate Disclosure

IR04 (Read only)

The Information within Live Facial Recognition (LFR) is accidentally or deliberately disclosed

inappropriately

IR04 Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR04 Severity 5 Very High | The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk

IR04 Risk Treatment Remote possibility, in the event occurred a Critical Incident Coordination Process would be implemented.

IR04 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR04 Current Severity 5 Very High | The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk.

IR04 Current Risk (Read only) 6

Information Risk 05 - Inappropriate Damage / Deleon

IR05 (Read only)

The Information within Live Facial Recognition (LFR) can be damaged or inappropriately deleted

IR05 Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR05 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR05 Risk Treatment Should the data on the USB device be damaged or destroyed, we control the originals, we can make another copy and log such accidental loss / destruction as a Security Incident.

IR05 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR05 Current Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR05 Current Risk (Read only) 3

Information Risk 06 - Integrity

IR06 (Read only)

The integrity of the Information within Live Facial Recognition (LFR) is jeopardised i.e. it can be

damaged/altered

IR06 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR06 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR06 Risk Treatment As the source images are extract from Force systems it is unlikely that this would occur unless the USB device became corrupt in transit, or during the encryption process.

IR06 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR06 Current Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR06 Current Risk (Read only) 3

Information Risk 07 - Inaccessibility

IR07 (Read only)

The Information within Live Facial Recognition (LFR) is inaccessible to those who should have access to it.

IR07 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR07 Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR07 Risk Treatment Occasionally, we will look to invite observes to view our operations to demonstrate the legitimacy of this process. This is to ensure transparency and mitigate any public fears. These people will be local elected officials or other known partners.

IR07 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR07 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR07 Current Risk (Read only) 2

Information Risk 08 - Utilisation

IR08 (Read only)

The Information within Live Facial Recognition (LFR) is not shared/utilised when it could/should be.

IR08 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR08 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR08 Risk Treatment Traditional Policing tactics would still exist.

IR08 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR08 Current Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR08 Current Risk (Read only) 3

Information Risk 09 - Located

IR09 (Read only)

The Information within Live Facial Recognition (LFR) cannot be found (e.g. physical documents or searching of IT)

IR09 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR09 Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR09 Risk Treatment ICT procedures in place, no physical documentation exists

IR09 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR09 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR09 Current Risk (Read only) 2

Information Risk 10 - Lawful

IR10 (Read only)

There is no lawful basis to hold or use the Personal Data held within Live Facial Recognition (LFR). Personal data is any information that identifies, or can be used to identify, a living individual – either on its own or when combined with other information.

IR10 Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR10 Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact.

IR10 Risk Treatment We know that we currently hold information beyond its retention date. However, the criteria for nominals who will be subject to the watchlists means it is highly unlikely images that we should no longer delete will be processed as part of this activity.

IR10 Current Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR10 Current Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact.

IR10 Current Risk (Read only) 5

Information Risk 11 - Transparency

IR11 (Read only) Personal Data held within Live Facial Recognition (LFR) is being used unfairly or without transparency to data subjects. Personal data is any information that identifies, or can be used to identify, a living individual - either on its own or when combined with other information.

IR11 Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR11 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR11 Risk Treatment LFR Policy documents details steps.

IR11 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR11 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR11 Current Risk (Read only) 2

Information Risk 12 - Incompatible

IR12 (Read only)

Personal Data held within Live Facial Recognition (LFR) is being used for a purpose incompatible with the reason it was first used/collected. Personal data is any information that identifies, or can be used to identify, a living individual - either on its own or when combined with other information.

IR12 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR12 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR12 Risk Treatment LFR Policy documents details steps.

IR12 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR12 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR12 Current Risk (Read only) 2

Information Risk 13 - Pseudonymisation

IR13 (Read only)

Pseudonymised versions of the information held within Live Facial Recognition (LFR) can be altered to identify individuals. Pseudonymisation is processing personal data so it can't be linked to an individual without separate, protected additional information.

IR13 Likelihood 0 Zero Chance | Not Applicable

IR13 Severity 0 Not Applicable

IR13 Risk Treatment Data is not anonymised.

IR13 Current Likelihood 0 Zero Chance | Not Applicable

IR13 Current Severity 0 Not Applicable

IR13 Current Risk (Read only) 0

Information Risk 14 - Inaccurate or Incomplete

IR14 (Read only)

The information held within Live Facial Recognition (LFR) is inaccurate or incomplete

IR14 Likelihood 4 Realistic Possibility | Between 1 in 2 and 2 in 5 or 40-50%

IR14 Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact.

IR14 Risk Treatment Data is taken from the source system, which identifies suspects based on identification procedures. The risk sits with the source system and there are extensive safeguards in place. It is extremely unlikely, however not impossible, that we may currently hold an image past the point of which it should have been destroyed. This issue has been addressed by ICT and any such image will not be in the cohort of images which will be uploaded to the LFR computer. The quality of the data contained within the watchlists are dependent of the data quality of the source system. It is to be expected that there could be data quality issues as a result.

IR14 Current Likelihood 4 Realistic Possibility | Between 1 in 2 and 2 in 5 or 40-50%

IR14 Current Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact.

IR14 Current Risk (Read only) 7

Information Risk 15 - Correction

IR15 (Read only)

The information held within Live Facial Recognition (LFR) cannot be amended or corrected when it needs to be.

IR15 Likelihood 0 Zero Chance | Not Applicable

IR15 Severity 0 Not Applicable

IR15 Risk Treatment. The LFR images are uploaded / refreshed prior to each operational use. Therefore, they can always updated / corrected.

IR15 Current Likelihood 0 Zero Chance | Not Applicable

IR15 Current Severity 0 Not Applicable

IR15 Current Risk (Read only) 0

Information Risk 16 - Duplication

IR16 (Read only)

Records Management - Duplicate versions of the information held within Live Facial Recognition (LFR) exist

IR16 Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR16 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR16 Risk Treatment Data is constantly monitored and duplicate records are merged when discovered, however the presence of a duplicate record would not adversely impact the LFR process. It is extremely unlikely, however not impossible, that we may currently hold an image past the point of which it should have been destroyed. This issue has been addressed by ICT and any such image will not be in the cohort of images which will be uploaded to the LFR computer.

IR16 Current Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR16 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR16 Current Risk (Read only) 3

Information Risk 17 - Excessive

IR17 (Read only)

Excessive information is held within Live Facial Recognition (LFR)

IR17 Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR17 Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR17 Risk Treatment Each watchlist is compiled from pre-determined characteristics. There is a chance unwanted data is used on the watchlist, but this is remote and real world consequences even more remote.

IR17 Current Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR17 Current Severity 2 Low | The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered.

IR17 Current Risk (Read only) 4

Information Risk 18 - Destruction

IR18 (Read only)

The information stored within Live Facial Recognition (LFR) is held longer than is necessary or cannot be deleted/disposed of when no longer required

IR18 Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR18 Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR18 Risk Treatment Automatic deletion is in place for the Biometric data on the LFR. There is a documented manual deletion confirmation in place for the USB device, including a signed form.

IR18 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR18 Current Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR18 Current Risk (Read only) 4

Information Risk 19 - Training

IR19 (Read only)

The users of Live Facial Recognition (LFR) are inadequately trained in its use

IR19 Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR19 Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR19 Risk Treatment Training regime in place and only trained persons would be involved in compiling the watchlist or operating the system.

IR19 Current Likelihood 2 Highly Unlikely | Below 1 in 5 or 20%

IR19 Current Severity 3 Medium | The consequences of this risk materialising would have a moderate impact on day-today delivery. Some immediate action might be required to address risk impact, plus the development of an action plan.

IR19 Current Risk (Read only) 5.

Information Risk 20 - Governance

IR20 (Read only)

There is inadequate governance for the information within Live Facial Recognition (LFR) (e.g. lack of policy or procedure surrounding the access or use)

IR20 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR20 Severity 5 Very High | The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Some immediate action is required to mitigate the risk.

IR20 Risk Treatment Policy approved at SMB in December 2025.

IR20 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR20 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR20 Current Risk (Read only) 2.

Information Risk 21 - ISA / DPC

IR21 (Read only)

There is an absence of an adequate Information Sharing Agreement or Data Processing Contract (where one is required) for the information within Live Facial Recognition (LFR)

IR21 Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR21 Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR21 Risk Treatment No data sharing takes place. Data is already in Merseyside Police's possession from source system. Currently we will be loaning SWPs LFR assets (as part of mutual aid) and providing our data, to be used with said asset.

IR21 Current Likelihood 1 Remote Chance | Below 1 in 20 or 5%

IR21 Current Severity 1 Very Low | The organisation accepts this risk / impact of risk would be insignificant.

IR21 Current Risk (Read only) 2

Information Risk 22 - Discriminatory

IR22 (Read only)

The information within Live Facial Recognition (LFR) is inappropriately discriminatory

IR22 Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR22 Severity 4 High | The consequences of this risk materialising would be severe but not disastrous. Some immediate action is required to mitigate the risk, plus the development of a comprehensive action plan.

IR22 Risk Treatment There is potentially disproportionality in the application of police powers, thus resulting in disproportionality in the data held and used within the LFR system. There are multiple strands of work to reduce this disproportionality.

IR22 Current Likelihood 3 Unlikely | Below 1 in 3 or 35%

IR22 Current Severity 4 High | The consequences of this risk materialising would be severe but not disastrous. Some immediate action is required to mitigate the risk, plus the development of a comprehensive action plan.

IR22 Current Risk (Read only) 7.

Step 7: Approvals

Highest Current Risk (Read only)

7 ISO

ISO or ITSO Approval (Where highest Current Risk is below 8)

ISO Caddick Phillip James

ISO Comments - I have conducted a comprehensive review of this DPIA in collaboration with Ian Boyham, our Force Data Protection Officer. Throughout our discussions, we meticulously examined the various risk factors associated with Live Facial Recognition (LFR). Both Ian and I are confident that the risk levels identified are manageable and fall within acceptable parameters. However, it is important to note that, despite the risk scores being below the threshold required for Information Asset Owner (IAO) sign-off, we anticipate that this DPIA may attract scrutiny in the future. Given the heightened public interest in facial recognition technology, we believe it is prudent to ensure thorough documentation and review at this stage.

Category Full

Information Asset Owner Approval (Only required if highest Current Risk is 8 or 9 after migration)

IAO Thornton Zoe

IAO Comments - I am the sponsor of this Live Facial Recognition DPIA, and the Senior Responsible Officer and Information Asset owner. On several levels it is vital that I am confident that we are able to protect the information assets that I am responsible for. This DPIA along with the technical and procedural aspects of going live with LFR have been carefully worked through with Subject MaRer Experts. I am confident of the mitigation in place to address the risks presented. This DPIA is a living document and as a part of the debriefing process any issues will be identified and addressed whether this be in a test or live environment.

Senior Information Risk Owner Approval (Only required if highest Current Risk is 10, or above, after migration)

SIRO Enter a name or email address

SIRO Comments

Data Protection Officer Approval

DPO Boyham Ian Frank

DPO Comments As outlined by Phillip Caddick above, we can realistically expect to be challenged via FOI or other regarding our use of this technology in the future. I believe all the risks have been sufficiently covered as part of this DPIA. While the issue regarding retention of material that should be have been to RRD remains a factor and the Force should have a long-term plan for this, I believe there is a low risk that this information will form part of any watchlists.

Information Commissioner's Office (ICO) Consultation

ICO Contact made aware of deployment

ICO Comments

Enter value here

ICO Reviewer

Enter value here

Version History

Version Number	Date	Detailed rational behind amending/updating policy or procedure.	Policy Owner Details	Policy Author Details
1	12/12/2025	Document Created	Ch/Supt Thornton	DPO Ian Boyham Sgt 7649 Hilton

If you need this information in an accessible format, please contact us via our website or call 101