DPIA Ref:
Police Force:

Data Protection Impact Assessment (DPIA)

You should start to fill out this template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated into your project plan. Please provide as much details as possible, avoiding jargon or acronyms where possible

Controller details

Name of Force	South Wales Police (SWP)
Subject/Title of DPIA	Live Facial Recognition (LFR)
Name of DPO	Louise Voisey

Project Name	Live Facial Recognition
Responsible Owner	Chief Inspector Scott Lloyd
Business Area/Department	Digital Services Division
Proposed implementation date	09.08.2022
Version No.	0.6

It is recommended that you refer to the DPIA guidance and process documents (hyperlink) to assist in the completion of these sections.

Terms & Definitions: Capitalised terms used within the SWP LFR DPIA shall have the meaning given to them in section 3 of the SWP LFR Policy document and Annex B of the DPIA unless otherwise defined.

Step 1: Project Aims and Processing

Explain what the project or processing aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents

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

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

- supporting the location and arrest of people wanted for criminal offences
- preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders)
- supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc)

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

Compiling/using existing database of images: the LFR application requires a Watchlist of reference images against which to compare facial images from the video feed. 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 SWP LFR Policy outlines considerations relevant to lawfully compiling a Watchlist including determining which persons may be on a Watchlist and the sources of Watchlist imagery.

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

Personal data: Outline what categories or personal data will be processed and explain why each is necessary to achieve the project aims. *E.g. names, addresses, DoBs, criminal records, unique identifiers such as IP addresses, usernames, e-mail addresses*

Personal data which is already accessible and processed by the police (held in source system Niche RMS) 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 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.

Special Category data: please select all applicable categories below which will be processed

☒ Race

☒ Ethnic origin

☐ Political opinions

☐ Sex life

☐ Religion

☐ Philosophical beliefs

☐ Trade union membership

☐ Genetic Data

☒ Biometric Data

☐ Sexual orientation

☐ Health

☐ None

Potentially these categories of data may be processed which in turn may indicate an individuals 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.'

It should be noted that processing personal information as part of an FRT Equitability Evaluation will be detailed in a separate DPIA.

Data Subjects: What categories of data subject are involved?

x Persons suspected of having committed or being about to commit a criminal offence
x Persons convicted of a criminal offence
x Persons who are or may be victims of a criminal offence
x Witnesses or other persons with information about offences
x Children or vulnerable individuals
x Police officers or staff (current and former)
x 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.

Step 2: Describe the processing

Describe the nature of the processing: How will you collect use, store and delete data? What is the source of the data? Will you be sharing with anyone? Consider the end to end process and provide these details for each step of the process.

If possible, please include/attach a flow diagram or infographic.

What types of processing identified as high risk are involved?

Will you be collecting new information about individuals?

The technical operation of LFR comprises the following six stages:

(1) Compiling/using an existing database of images. LFR requires a database of existing facial images (referred to in this case as a Watchlist) against which to compare facial images and the biometrics contained in them. For such images to be used for LFR, they are processed so that the "facial features" associated with their subjects are extracted and expressed as numerical values.

(2) Facial image acquisition. A CCTV camera takes digital pictures of facial images in real time. This case is concerned with the situation where a moving image is captured when a person passes into the camera's field of view, using a live feed.

(3) Face detection. Once a CCTV camera used in a live context captures footage, the software
(a) detects human faces and then
(b) isolates individual faces.

(4) Feature extraction. Taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face, the resulting Biometric Template being unique to that image.

(5) Face comparison. The 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 Negaive 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:

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

Images are typically imported in to the LFR application for each Deployment from NICHE RMS 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:

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.

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:

a. using LFR to facilitate their location is necessary to manage the risk of harm identified; and
b. 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 SWP 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;

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

It is the intention during each Deployment to allow the LFR application to enrol and therefore process as many individuals as possible, however 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.

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
- 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

Describe the scope of the processing: How much data will you be collecting and using? How often? How long will you keep it? How many individuals' data will be involved? What geographical area does it cover?

Typical Deployments 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 contractual limit is currently 2,000 images.

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

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 three 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

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.

Whilst LFR may be used at locations across South Wales, 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 (as more particularly outlined in SWP LFR Legal Mandate and SWP LFR SOP). These controls

assist the public and decision-making officers to understand LFR and foresee where it may be used.

Source System – Niche Record Management System

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

Non-conviction – upon request

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

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

Group 4 (missing persons) – 6 years then review

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

Group 1 - subject is 100 years the review

Group 2 – 10 year clear period then review

Group 3 – 6 year clear period

Group 4 (missing persons) – 6 years then review

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have over the processing of their data? Would they expect you to use their data in this way?

Do they include children or other vulnerable groups? Are there prior concerns or challenges over this type of processing or security flaws?

Is the processing new in any way? Are there any current issues of public concern that you should factor in?

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 will be utilised to publicise details of the Deployment.

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

Watchlists
Those included in the watchlist will be 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.

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.

Where it is necessary, proportionate, in pursuit of a legitimate aim and in accordance with the law. The AO must be satisfied by the steps taken to ensure the composition of the Watchlist is not excessive and only includes those who need to be located by SWP using LFR on a strict necessity basis.

The LFR Operator has the ability to delete images from the Watchlist and will record such action in the operator log.

Children/Vulnerable Groups
It is possible that there will be processing of children or vulnerable groups however if their Biometric Template does not generate a Possible Match no other details will be processed and this information 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. 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.

Given the potential for System Factors relating to age, specific regard needs to be had to the importance of locating those aged under-18 on a risk-based approach in line with the SWP Documents, with a particular focus on ensuring the necessity case is fully made out.

If LFR is to be used to locate person aged under 13-years-old, specific regard should be had to anticipate LFR application performance issues. Specific advice must (at this time) be sought from Special Legal Casework and the SWP LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO.

Issues of concern 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 human failsafe of an officer checking the image when a Possible Match is received is 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. SWP and the NPCC are keen to continue to engage with the Home Office with regards the Department of Science, Culture, Media and Sport Data Reform Consultation.

Describe the purposes of the processing: what do you want to achieve through the processing of this data? Will there be any impact on the individuals whose data is being processed?
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 duties, which include the prevention and detection of crime,

the preservation of order, and bringing offenders to justice.

The following are illustrative examples where LFR may assist 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.

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 SWP 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. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety. They could also include there being focus placed on ensuring the public understand the use of LFR is to help them safety undertake their assembly.

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.

Step 3: Consultation

Consider how to identify and consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

A number of stakeholders have been engaged from the outset of this project initially by South Wales Police 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 Commissioner's Office – Advice and guidance was received from the ICO. Opinion on deployment of Live Facial recognition in public places and interested party in *(on the application of Edward Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058*.

2. 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.

3. Defence Science and Technology Laboratory (DSTL) – With the provision of guidance on procurement, testing and Deployment of the technology, along with advice around academic documentation supporting the proof of concept of the product. They remain a critical friend to the project.

4. Home Office Biometric Programme (HOBs) – Additional guidance in support of the above from the HOB lead on PIA's.

5. South Wales Police Independent Ethics Committee – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.

6. The Metropolitan Police – Professional discussions around lessons learned over previous deployments, particularly the Notting Hill Carnival in the pursuit of a best practice model across forces.

7. Leicester Police – Professional discussions over their previous use of slow-time recognition functionality in the preparatory phase of our project implementation.

8. National Police Chiefs Council – Professional discussion and advice over the development of the project in its phases and the use of custody image.

9. The Surveillance Camera Commissioner/Biometric Commissioner – Professional discussion over project proposals and implementation. The SCC Code of Practice also states that an individual "can rightly expect surveillance in public places to be necessary and proportionate with appropriate safeguards in place". The Code and the guidance 'Facing the Camera' has been considered as part of the DPIA. Deployments of LFR also incorporate the SCC's checklist.

10. The College of Policing – Professional discussion over deployment of an LFR APP

11. Police Digital Service – Professional discussions over system developments against a desired national rollout picture of the future.

12. The National Physics Laboratory – Professional discussions integrating academic research into the policing technology, the ethical dilemmas associated with it and its deployment.

13. National Law Enforcement Database Programme (NLEDP) – Guidance in support of new platform anticipated 2023.

14. Ada Lovelace Institute – a report commissioned in September 2019 indicated that public support for LFR would be conditional on a demonstrable impact on reducing crime – 71% agreed with the statement "the police should be able to use facial recognition on in public spaces, provided it helps reduce crime".

15. The London Policing Ethics Panel (PEP) – an independent body set up by the mayor to provide advice on ethics, which produced a report on the LFR trials conducted by the Metropolitan Police. The report included the results of a public survey which showed:

- 57% of those surveyed felt police use of LFR is acceptable;
- public support increases to 83% acceptance for LFR to search for serious offenders;
- 50% of those surveyed feel that the technology would make them feel safer; *and*
- approximately one third raised concerns about the impact on their privacy.

The legality of the use of LFR in a public place was also the subject of civil court proceedings in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)* and subsequently in the Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 which concluded:*

"…….the legal framework which regulates the deployment of AFR Locate does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary."

And that to be in accordance with the law the legal basis must:

"be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself".

16. Publication consultation sessions have been completed at various locations across South Wales Police force area over a four-year period. These have culminated in workshops delivered at SWP HQ. There has also been public consultation during each deployment of the technology. Public consultation will be ongoing and has been deemed particularly successful when LFR is deployed where an opportunity exists to demonstrate the technology.

17. Participation by Chief Constable Jeremy Vaughan in the SCC/BC event 'Is there a legitimate role for facial recognition in policing and law enforcement' at the London School of Economics on the 14th June 2022. Attendance included academics, technologists, representation from civil libertarian groups and broader society.

Step 4: Lawfulness, Necessity and Proportionality

Please provide information on following requirements or seek advice from the DPIA adviser or DPO:	
Is the processing for Law Enforcement Purposes or general processing? ICO Guidance on Law Enforcement Processing and General Processing	Both

<table>
<tr><td>Legal power to carry out processing e.g. statute, common law, court order etc. (please provide details)</td><td colspan="2">Common law – policing purpose and law enforcement purpose.
Police and Criminal Evidence Act 1984

The LFR Legal Mandate provides detailed analysis relating to article 8 of the Human Rights Act and other relevant legal considerations.</td></tr>
<tr><td>Lawful basis for processing (please select the appropriate conditions. If different conditions apply to different stages of the processing please provide further details)

General Processing (GDPR):
Please select one condition for processing personal data. If processing special category data please select a further condition.

ICO Guide to GDPR - Lawful Conditions for processing

Law Enforcement Processing:
Please select one condition for processing personal data only.
If sensitive processing takes place please select a further condition.

ICO Guide to Law Enforcement Conditions</td><td>General: Personal data

☐ Consent
☐ Contract
☐ Vital Interests
☐ Legal Obligation
X Public Task
☐ Legitimate Interests</td><td>General: Special category data

Explicit Consent
☐ Obligations & rights in employment, social security & social protection law
☐ Vital interests
☐ Members of former members of a not for profit body
☐ Data has been made manifestly public by the data subject
☐ Legal claims
X Substantial public interest
☐ Health
☐ Public interest in Public Health
☐ Archiving
X Historical research</td></tr>
</table>

	Law Enforcement: Personal data ☐ Consent X **Processing is necessary for the performance of a task carried out for that purpose by a competent authority.**	**Law Enforcement: Sensitive processing** ☐ Consent X **Processing is strictly necessary for the law enforcement purpose; and** **X Statutory etc purposes** **X Administration of justice** **X Protecting vital interests** **X Safeguarding of children and individuals at risk** ☐ Personal data already in the public domain ☐ Legal claims ☐ Judicial Acts X Archiving
Data Protection Act 2018 (to be completed where special category data (part 2) or sensitive processing (Part 3) is being carried out	Schedule 8 (Part 3) para 1 – Statutory purposes Schedule 8 (Part 3) para 2 – Administration of Justice Schedule 8 (Part 3) para 3 – Protecting the individual's vital interests Schedule 8 (Part 3) para 4 – Safeguarding of children and individuals at risk Schedule 8 (Part 3) para 8 – Preventing fraud Article 9 (Part 2) para 2a – Explicit consent Article 9 (Part 2) para 2g – Substantial public interest ○ Part 2 Schedule 1 para 6 Statutory ○ Part 2 Schedule 1 para 18 Safeguarding of children or individuals at risk ○	

Privacy Information – what information will you provide to the individuals whose data is being processed, how will this information be provided and at what stage of the processing activity. If no privacy information is to be provided, please provide the reason for this.	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. An overview of documents available to the public is at Annex A
Will the personal data collected be used for any other purposes? (*Please provide details)*	No.

Will the processing include mechanism to facilitate the exercise of individual rights *(please select which rights can be exercised)*	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. SWP 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.

How will you ensure that the data being processed is accurate and up-to-date? Accuracy Will the processing allow you to erase or rectify inaccurate data without delay?	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 SWP LFR application will not be more than 24 hours old to provide increased assurance that those on the list remain of interest to SWP. 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 SWP 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 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 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 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 SWP has 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 will assist 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. SWP currently use 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 SWP 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 SWP provides for an

	ongoing evaluation and a post Deployment review process on a per Deployment basis. The SWP supplier has also been held in high regard by the NIST in its 2018 evaluation of over 200 algorithms. SWP 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.
Does the processing require you to keep the information in an identifiable form? *(If yes, please provide reasons for this)* Could you pseudonymise or anonymise the data to achieve your aim?	The only information which is retained will need to be identifiable so that the policing purpose/law enforcement purpose can be fulfilled. Any retention beyond a Deployment will be in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or* in accordance with SWP's 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 to the Biometric Templates of members of the public captured by LFR. Where there is no match to the Watchlist the image will be deleted. The images on the Watchlist need to be identifiable to the police and cannot be anonymised or pseudonymised to achieve the aim of the Deployment.

How long do you need to retain the personal data? *(Please indicate the framework under which retention is stated)* What mechanisms are in place to review, dispose of, or delete the data when no longer required?	**Biometric Templates – no matches** Any Biometric Templates which do not match those on the Watchlist are automatically 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 three thumbnail images will be saved within the LFR 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 **LFR Operator and Engagement logs** Retained in line with MOPI retention periods. **CCTV Footage** All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained: • in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or* • in accordance with South Wales Police's complaints / conduct investigation policies. **Source System – Niche Record Management System** – MOPI retention period depending on suspected offence

	All personal data will be stored in accordance with MOPI standards – tier 1 for 31 days, tier 2 for 6 years plus 1, with tier 3 retained for one hundred years.
What organisational and technical measures will be in place to protect the personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage? How will you monitor the ongoing effectiveness of the security measures? *Note – if you are using data processors what guarantees will you obtain about their ongoing ability to keep the data secure?	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 SWP 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 SWP 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. *Chief Officers must establish their own Internal Governance arrangements for LFR. This should involve Chief Officer and PCC (or equivalent) oversight with separation from operational decisions/decision makers where possible to ensure sufficient independence and rigour when reviewing a Force's use of LFR. Forces should also seek to engage with ethics committees, where they exist in forces and may meaningfully be consulted in the first instance to help relevant oversight arrangements determined.* *When considering the ethical deployment of LFR, Chief Officers should consider the adoption of an ethical framework within which they will operate.* *See associated SWP LFR Documents* Criteria for a Deployment is specified in the SWP LFR Policy:

	Each Deployment must be appropriately documented, assessed and authorised. Where an AO is not immediately able to provide their decision in relation to an application to use LFR in writing their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable and, unless urgent, prior to the Deployment of LFR. The Deployment must be: ▪ targeted ▪ intelligence led ▪ time bound and geographically limited Compliance is demonstrated via force policy documents including: An **appropriate policy document** outlining the safeguards and controls in place **Assessments** - These include a Community Impact Assessment, an Equality Impact Assessment (or other similar documented record), an overarching Data Protection Impact Assessment, and the Surveillance Camera Commissioner's Self-Assessment. These documents need to be considered by the decision-maker when authoring an authority to ensure they are sufficient to address the issues arising from the proposed Deployment. The decision maker must involve their Data Protection Officer in

	writing the Data Protection Impact Assessment and in managing the processing of personal data. The decision-maker must ensure that 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 an intelligence case. The application should set out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, 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 written approval must be retained in accordance with **Information Management Authorised Professional Practice (APP)** and other relevant legislation or policy and be made available for independent inspection and review as required **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. **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. The processing will also take place against the requirements of the Surveillance Camera Code of Practice which has the following principles: 1. 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. 2. 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. 3. 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. 4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. 5. 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. 6. 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. 7. 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. 8. 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. 9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

	10. 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. 11. 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. 12. 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. The LFR uses an independent system to the current SWP technical architecture with 2 layers of password protection to access the application. The system is physically protected when in use. 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. The data is held securely on SWP systems accessible to SWP officers and staff which is fundamentally permission based. Officers leaving SWP automatically have their account disabled and therefore would no longer have access to the information. The data held on SWP 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 the individual identified as a Possible Match will be engaged by an Engagement Officer before any further action is taken. The use of LFR as a tool to locate Persons of Interest to SWP will be considered alongside other policing tools and tactics. 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. SWP LFR Documents provide for the training of officers and staff involved in LFR Deployments to be principally delivered by a DSD trainer. The training helps ensure role specific: 1. familiarity with SWP LFR Documents; 2. knowledge of Deployment processes; 3. understanding of the lawful processing of personal data in accordance with the Data Protection Act 2018; 4. understanding the scope of the Regulation of Investigatory Power Act 2000; 5. knowledge of police powers and how they may apply when responding to Alerts; 6. knowledge of how to configure the LFR application to maximise system performance, and how to minimise impact on others; 7. understanding of the characteristics of the LFR application that affect the likelihood that an Alert is reliable.

	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. More generally, SWP Senior Responsible Officer for LFR has directed that the False Alert Rate should be kept within a 1 in 1000 level to minimise the impact on the passing public whilst balancing the policing need to locate those on a Watchlist.
Will the personal data be held or transferred outside of the UK? *(If yes, please provide details of the location, the environment in which it will be held, reason for transfer and safeguards)*	No.
Will there be an information sharing agreement or contract in place with all parties with whom personal data will be shared? *Please provide details)*	Information will only be shared where necessary for a policing purpose on a case by case basis therefore no agreement is necessary. A contract will be in place with the algorithm supplier The supplier does not have routine access to the software and algorithm supplied to SWP and do not act as a data processor for the purposes of this DPIA.

Step 5: Identify and assess privacy & compliance risks

No.	Identify risk – Cause, event, effect	Likelihood	Impact	Overall risk
		L,M,H	L,M,H	L,M,H
1	As a result of the Watchlist being deleted after 24 hours the force may be unable to comply with a subject access request from a data subject resulting in complaints, reputational damage and potential financial claims.	L	M	L
2	There is a risk that intervention may take place as the result of a False Alert due the Threshold value for a Similarity Score being set too low or too high resulting in reputational damage, potential enforcement action and financial penalties, loss of public trust and increased volumes of complaints.	L	H	M
3	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
4	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
5	As a result of issues to narrow the scope of the Watchlist there is a risk that the images included for a Deployment may be excessive.	M	M	M
6	As a result of limited availability of images for testing the software there is a risk that bias may not eliminated in the algorithm resulting in a disproportionate number of individuals with protected characteristics being identified in False Alerts leading to potential legal challenge, financial claims and increase in complaints.	M	H	H
7	As a result of the wide-ranging capability of LFR to process large amounts of personal data	M	H	H

	there is a risk that the processing of personal data may be excessive resulting in regulatory action.			
8	There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action.	H	H	H
9	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
10	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
11	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
12	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
13	As a result of inconsistent guidance around the use of LFR there is a risk that officers may	H	H	H

	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.			
14	There is a risk that officers involved in the Deployment of LFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the Deployment of LFR and potential breaches of the DPA'18 which may result in enforcement action, legal action and financial penalties.	M	H	M
15	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
16	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
17	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

Step 6: Identify measures to reduce risk

No.	Measure to reduce or eliminate risk	Risk Treatment	Residual Risk	Measure approved
		Reduce Eliminated Accepted Transferred	L,M,H	Y/N
1	The Watchlist can be re-engineered. This can now be achieved via Niche RMS 'back-end' database by recording the nominal	Eliminated	L	

	number of an individual extracted into a Watchlist for any given date			
2	The LFR Operator will complete the Adjudication prior to any Engagement.	Reduced	L	
3	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	
4	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	
5	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	
6	Assurances around the testing conducted by the software supplier are required in the contract and is continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified as part of the public sector equality duty and through assessment by	Reduced	L	

	academic institutions, technology vendors and government opinion. Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented. Equality Impact Assessments will be completed and regularly reviewed against legal developments.			
7	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.	Reduced	L	
8	An additional legislative safeguard is any covert surveillance will require authority under the Regulation of Investigatory Powers Act 2000 as per arrangements for any covert surveillance.	Eliminated	L	
9	SWP 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	
10	Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. No Engagement will be made without checks being made on Possible Matches without manual intervention to reduce any damage and distress.	Reduced	L	
11	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	
12	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	

13	SWP 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 Practise that must be adhered to.	Reduced	L	
14	As part of the LFR training appropriate data protection training will be provided.	Reduced	L	
15	All SWP staff/ officers are trained in respect of the GPMS. 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	
16	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 SWP working with other police forces, law enforcement bodies and other agencies to assist SWP in discharging its common law policing powers. This action will not require the sharing of biometric data but may require SWP to share personal data, as it would for any investigation, in accordance with SWP's 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	
17	The technology has been trialled and tested by SWP. NEC algorithms have also been evaluated by NIST and the Department of Homeland illigitamate and SWP pays regard to these findings. An LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance	Reduced	L	

	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. SWP 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 SWP's use of LFR is reviewed by way of the post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.			

Step 7: Sign off and record outcomes

Action	Name, position, date	Notes
Measures approved by:	Chief Inspector Scott Lloyd 29.07.2022	Actions must be integrated back into the project plan with completion dates and action owners
Residual Risks approved by	Chief Inspector Scott Lloyd 29.07.2022	If accepting residual high risks, refer to DPO to consider ICO consultation before proceeding

DPO advice provided	Louise Voisey, DPO, 03.08.2022	DPO to advise on compliance, mitigating measures and whether processing can proceed
Summary of DPO advice: I am satisfied that all data protection considerations have been given to the application of LFR Deployments by SWP, with the benefit of insight from the regulators and the courts as to their expectations in terms of lawfulness and privacy. If there is a significant change to the way in which SWP conducts LFR deployments this DPIA should be revisited to take int consideration any new privacy risks to those whose details may be used or captured in future deployments. That is not to say that in each deployment all considerations should be applied to take into account the circumstances, necessity and proportionality of who and where it will include.		
DPO advice accepted or overruled by:	Advice accepted by Chief Superintendent Simon Belcher 09.08.2022	If overruled, an explanation must be provided.
Comments:		
Consultation responses reviewed by:	Chief Inspector Scott Lloyd 29.07.2022	If the decision does not align with the views of the consultees please explain
Comments: Document produced in response to information provided by stakeholders		
This DPIA will be kept under review (no later than on an annual basis) by:	Inspector Benjamin Gwyer FRT lead	The DPO should also review ongoing compliance with DPIA.

Annex A – Information Available to the Public

SWP has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of SWP 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, SWP has adopted a number of measures to ensure that the right to be informed is upheld.

A key measure is the publication of SWP's Privacy Notice, SWP policy on protecting special category and criminal convictions, and key SWP LFR Documents on the SWP website. Whilst SWP 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 SWP, as a public body, operates to. In doing so, SWP provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist. In this way, SWP's use of LFR is both foreseeable and assessable. The published documents provide information as set out in the table below.

Key documents available to the public	**Information included**
SWP Privacy Notice:	• Data Controller identity and contact details • Data Protection Officer details • The scope and purposes for processing personal data by SWP • 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).
SWP policy on protecting special category and criminal convictions	• SWP approach in relation to protecting and processing special category and criminal convictions data in relation to the data protection principles • The responsibilities of the Data Controller • Information relating to erasure and retention

	• How further information may be sought.
SWP LFR Legal Mandate	• The lawful basis for processing data in relation to LFR. Including in relation to: o Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Protection of Freedoms Act 2012 o Data Protection Act 2018 o UK General Data Protection Regulation o Freedom of Information Act 2000
SWP Policy Document	• An outline, strategic intent and objectives for the use of LFR and how personal data will be used by the LFR applciation • Key terms used across SWP LFR Documents • Data retention periods applicable to LFR
SWP LFR Standard Operating Procedure Processes	• Outlines measures relevant to considering when and where LFR can be Deployed by SWP. • 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: o signs publicising the use of the technology must be prominently placed in advance (both outside and within) the Zone of Recognition; and o 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 SWP website for more information.
SWP 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.
SWP 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 General Data Protection Regulation • Explains how SWP complies with the Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of personal data.

Annex B – LFR Terminology

Within SWP and throughout the SWP LFR Documents, 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 (similarity) 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.

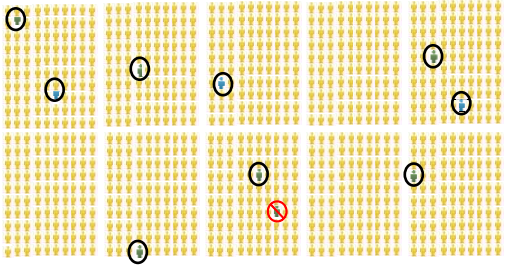
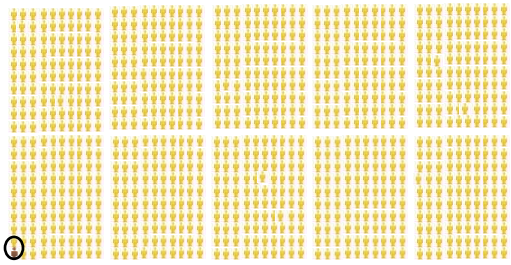
False Alert
When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement.

(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 officer 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:

a. location
b. dates and times
c. deployment and watchlist rationale
d. legal basis
e. necessity
f. proportionality
g. safeguards
h. watchlist composition
i. authorising officer
j. resources
k. relevant statistics
l. outcomes
m. 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 SWP deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of SWP 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 being of sufficient similarity above the threshold.

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.