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) / Gwent Police (GWP)
Subject/Title of DPIA	Operator Initiated Facial Recognition (OIFR)
Name of DPIA adviser	Louise Voisey

Project Name	Facial Recognition Technology (FRT)
Responsible Owner	Chief Inspector Scott Lloyd
Business Area/Department	Digital Services Division
Proposed implementation date	
Reference No. *(to be allocated by IM)*	

Terms & Definitions: Capitalised terms used within this OIFR DPIA shall have the meaning given to them in section 3 of the OIFR Policy Document 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

Operator Initiated Facial Recognition

The use of facial recognition where:
(i) media is directly captured of a Subject present; or
(ii) media is otherwise acquired in lieu of capturing it,

with the intent of subjecting it to analysis by the FRT System. The results of such analysis could shape events to which the footage relates in real time.

In SWP/GWP this consists of a mobile phone (OIFR Device) deployment of FRT technology, which compares a photograph of a person's face taken on a mobile phone which is processed to create Biometric Template which is then compared with the Biometric Template from images contained in the Image Reference Database(s) in order to assist an Operator identify a Subject.

The collection of personal information is via the Operators OIFR Device which is built with force accredited security to protect data, principally using two factor authentication to the device and a Virtual Private Network (VPN). There is an auditing capability to prevent unauthorised access or misuse. When a Subject refuses to comply with an officer's legitimate request for their details the Operator will take a photograph on the device i.e. the "Probe Image". The OIFR Device will send the image to the FRT System which is a static server which runs the FRT software, where a Biometric Template will be generated of the individual's face, this will then be compared to other Biometric Templates of images located in the Image Reference Database(s).

The Probe Images are submitted via SWP/GWP bespoke application (iPatrol) and are not saved within the Operator's OIFR Device gallery and are immediately and automatically deleted.

The Probe Image will be sent via secure transmission (via iPatrol) to the FRT System and compared against the Image Reference Database(s).

When will OIFR be used?

OIFR will not be used to replace traditional means of identification, such as having a conversation with the individual who then provides their name which is checked against police indices to identify them. Wherever possible, it must only be used after an interaction has occurred between the Operator and that Subject and it has not been possible to identify the Subject by usual police means such as that described.

OIFR can only be utilised if both a **reason for use** and **grounds for use** exists.

Reasons for use

Use of OIFR will only occur when the identity of a Subject is not known and at least one of the following reasons for use applies:-

1. The Subject is unable to provide their details (deceased, unconscious, incapacity through drink or drugs, mental health or age barriers)

2. The Subject has refused to provide their details.

3. It is reasonable suspected that the Subject has provided false details.

'The Subject is unable to provide their details'. If the Subject lacks capacity to provide their details due to mental health or age barriers or there is a clear language barrier preventing this being achieved, the Operator is to undertake reasonable lines of enquiry (such as the identification of an appropriate carer or the utilisation of language line) in order to facilitate identification prior to use of OIFR.

Grounds for use

Secondly, OIFR can only be used for a policing purpose when one at least of the following applies.

Is suspected to be : -

1. Wanted by the courts.

2. Of having committed a criminal offence or is unlawfully at large with further police action required.

3. Subject of bail conditions, court order or other restriction that would be breached if they were at the location at the time.

4. Missing persons deemed increased risk.

5. Presenting a risk of harm to themselves or others.

6. Subject is deceased or it has been confirmed that they are deceased

'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 to further policing enquiries. On other occasions, the investigation may, for example, require details to be verified with an individual to progress the investigation.
Missing persons deemed increased risk'. This term will be subject to the College of Policing definition of medium risk (or above). 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 reflect that using OIFR is necessary to manage the risk of harm identified and police action is required in order to manage the risk of harm.

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

- supporting the identification and arrest of people wanted for criminal offences
- supporting the identification 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 OIFR comprises of the following six stages:

Compiling/using existing database of images: OIFR requires an Image Reference Database(s) of images against which to compare a facial image submitted from the Operator's OIFR Device. In order for images to be used for OIFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template).

Facial image acquisition: A digital image submitted from the Operator's OIFR Device whilst utilising OIFR.

Face detection: Once the image has been submitted to the FRT System it detects individual human faces.

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

Face comparison: The FRT System compares the Biometric Template with those held on the Image Reference Database(s).

Matching: When the facial features from two images are compared the FRT System generates a Similarity Score. This is a numerical value indicating the extent of similarity

between the Probe and Candidate Image, with a higher score indicating greater similarity. The top six similar Candidate Images are returned to the Operator. In this way, OIFR 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), retrospective facial recognition may be used after an event to help officers establish who a person is or whether their image matches against other media held on databases. Also, Live Facial Recognition (LFR) which is the use of overt facial recognition to locate people on a watch list who are sought by the police.

There are separate DPIAs for RFR and LFR.

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 already processed by the Police will be processed in conjunction with the use of OIFR including name, date of birth, address however these details will not be included in the actual OIFR use of facial recognition technology but would be processed upon the return of the Candidate Images and therefore should be considered outside the scope of this DPIA.
Personal data in respect of individuals to are to be included in the Image Reference Database 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 as part of OIFR although algorithms will be developed and continuously tested 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.'

Data Subjects: What categories of data subject are involved?

x Persons suspected of having committed a criminal offence
x Persons convicted of a criminal offence
x Children or vulnerable individuals
x Police officers or staff (current and former)
x Other

If other, then please provide further details below:

A Biometric Template of the Probe Image captured by OIFR and therefore a cross section of the general public including all categories will potentially be processed.

The Image Reference Database(s) will be compiled from custody images and missing persons images (deemed increased risk) based on the criteria for the deployment.

It is possible that the personal data of individuals aged under 18 years, a person with a disability or vulnerable adults will be processed where there is a policing need and it is deemed to be necessary and proportionate to identify 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 OIFR comprises the following six stages:

1. **Compiling/using existing database of images:** OIFR requires an Image Reference Database (s) of images (Candidate Images) against which to compare a facial image submitted from the Operators OIFR Device. In order for images to be used for OIFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template).

2. **Facial image acquisition:** A digital image submitted from the Operators OIFR Device whilst utilising OIFR.

3. **Face detection:** Once the image has been submitted to the FRT System it detects individual human faces.

4. **Feature extraction:** Taking the detected face the FRT System automatically extracts facial features from the image, creating the Biometric Template.

5. **Face comparison:** The FRT System compares the Biometric Template with those held on the Image Reference Database.

6. **Matching:** When the facial features from two images are compared the FRT System generates a Similarity Score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. The top six similar Candidate Images are returned to the Operator. In this way, OIFR works to assist the Operator make identifications rather than acting as an autonomous machine-based process devoid of user input.

Additional information is also created in the form of metadata i.e. time, date and location. Where a Subject is engaged by an Operator following a Possible Match other details such as Operator defined age, gender and ethnicity will be captured.

Initial testing of OIFR will include images of SWP staff with their consent, this is reflected in the lawful basis indicated below, however consent does not apply to the live use of

OIFR which will be conducted as part of the public task of the police and in substantial public interest.

Image Reference Database(s)

OIFR will utilise SWP/GWP custody images and images of missing persons (deemed increased risk). Image Reference Databases reside on the FRT System and not the Operators OIFR Device.

Images are imported into the FRT System from Niche RMS (SWP/ GWP records management system which includes all custody images and images of missing persons) sSee section 3 OIFR Policy). Data may also be provided by other police forces and agencies associated with law enforcement. During the OIFR pilot no other images other than custody images and missing person images (deemed increased risk) are considered for use.

Image Reference Database(s) are made up of the entire custody database for the SWP and GWP area. It also includes missing persons (deemed increase risk) for the SWP area. Image Reference Databases are a direct duplication of the images that are currently legitimately stored in Niche RMS, which is the source of custody and missing person images.

It has been considered whether there is a necessity to reduce the Image Reference Database further when considering different grounds for use or by Subjects based on demographic cohort.

When considering grounds for use it has been deemed necessary and proportionate to search all custody images or missing person images (deemed increased risk) as the intention for OIFR is to identify the Subject and to provide the Operator additional information relating to the Subject (i.e. warning markers) to effectively navigate the National Decision Model (NDM).

The exception could be for grounds 1-3, with ground 2 further delineated by suspicion for offences committed at or about the time of OIFR use or for suspicion of committing historical offences.

Searching of the entire custody database for offences that have occurred at or about the time OIFR is utilised may be necessary and proportionate as the purpose of the search is both to identify the Subject and to provide the Operator with additional information relating to the Subject (i.e. warning markers) to effectively navigate the NDM. These Subjects at the time of utilising OIFR would not be shown as a suspect within Niche RMS for the matter that is currently being considered by the Operator.

The primary purpose for OIFR use for suspicion of committing historical offences and Subjects for grounds 1 and 3 is to confirm whether the Subject is currently suspect for a

historical event. To that end it may be appropriate to limit the OIFR enquiry to Subjects associated with grounds 1-3 (i.e. limit the OIFR enquiry to Subjects with live warrants, suspects, bail conditions, etc) and thus significantly reducing the number of Candidate images searched against.

Due to the way in which Subjects are associated to a Niche RMS occurrence for grounds 1-3 it currently not technically possible to create an accurate sub-section of the custody Image Reference Database for Subjects for live warrants, suspects, bail conditions, etc.

Therefore, to ensure OIFR is effective when utilised for grounds 1-3 (ground 2 suspicion of historical offences) it is deemed necessary and proportionate to search the entire custody image database which will allow the Operator to manually interrogate the associated record to confirm or deny whether the Subject is currently suspected of an offence, wanted on warrant and subject to relevant bail conditions (i.e. grounds 1 -3).

It has also been considered whether there is an opportunity to further limit the OIFR search of the Image Reference Database(s) by further delineation based on the Subjects demographic cohort.

For example, it would be technically possible to delineate the Image Reference Database by age, gender and ethnic background. As such an Operator could then choose to limit the OIFR enquiry by association to a demographic cohort and thus reduce the Candidate Images searched against. An example of this would be only searching custody images of females if the Subject presented as female.

OIFR use will at times be utilised when Subjects are not engaging with the Operator, it would therefore be for the Operator to determine the demographic cohort of the Subject. A similar challenge may be presented when the Person of Interest attends at a custody suite for image capture.

This would potentially lead to a subjective decision by the Operator or custody staff which may unwittingly exclude relevant Persons of Interest from an Image Reference Database or a Subject searched against the incorrect Image Reference Database. For these reasons it has been deemed ineffective to reduce the Image Refence Databases by demographic cohort.

Upon go live for the FRT System a script has been run against Niche RMS to bulk enrol the custody images into the FRT System. Consideration has been given to automatically removing images of un-convicted persons but at this stage it is not possible due to the technical legacy build of the system.

SWP/GWP currently consider deletion of custody images captured of individuals relating to a non-conviction upon request – this issue is not limited to SWP/GWP. At present due to the size of the task to apply automatic deletion it has not been deemed proportionate

to manually remove non-convicted custody images from the Image Reference Database as this will negate the benefits of using the technology. However, no action is taken regarding an individual identified without human intervention.

When an individual has their custody image taken these will be 'seen' by the FRT System and ingested. Currently there is approximately a 5-minute time lag between Niche RMS and the FRT System.

Images Reference Databases do not reside on the Operators OIFR Device but are accessed using an interface with the FRT System which is located on SWP premises.

To ensure parity between the image library in Niche RMS and the FRT System each image is applied a hash value with the values being compared on a daily basis to identify any variance.

To that end when an individual successfully applies to SWP/GWP for a non-convicted custody process image to be deleted from Niche RMS the comparison of the hash values would effectively identify the inconsistency between the data sets and an alert email would be sent to the project team to ensure deletion from the FRT System.

Probe Images are submitted from the OIFR Device via a secure VPN using the cellular network to the FRT System, the Probe Images will not be saved in the FRT System. A Biometric Template is created from the Probe Image and compared against Biometric Templates of the Candidate Images.

Force policy documents should also provide that the composition of the Image Reference Databases:

a. 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 Image Reference Database; and
- is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Image Reference Database.

A record of the search (i.e. the attempt to match an image in the Image Reference Database) will not be available within the audit log of the FRT System. An automated record of the search will be saved in the Operator's Electronic Pocket NoteBook. This is

automatically logged and this will not include the Probe Image and the record will be saved in line with the MOPI retention period.

Effective auditing and accountability with regard to use of OIFR is of paramount importance to ensuring transparency and maintaining public confidence. In light of this, use of OIFR automatically generates an audit log which is recorded in the Operator's ePNB.

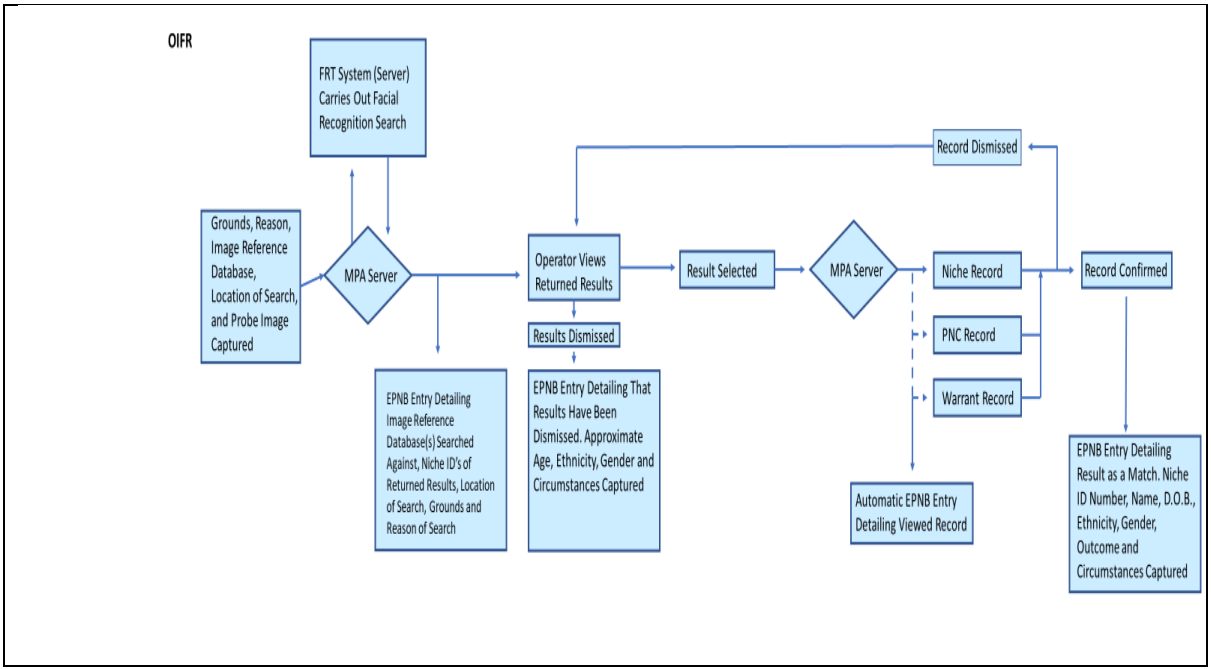
The automated completion of ePNB entries provides an audit function that allows use of OIFR to be automatically monitored and evaluated without the need to manually check Operators ePNB's.

Using the electronic pocket notebook the record of a search is fully auditable and the full record will include the Operator's rationale for using OIFR and a description of the Subject to include their age, gender and ethnicity which requires manual input by the Operator. The application will always return the six most similar Candidate Images to the Operator's OIFR Device. These images will not be saved in the Operator's Electronic Pocket NoteBook, instead the Niche RMS nominal number relating to the Subject will be saved as a reference back to the image selected by the Operator if necessary.

On receipt of the Candidate Images to the OIFR Device, no other personal information relating to the Subject will be available. The Operator will use his/her judgement to identify a Possible Match.

If the Operator considers a Possible Match has been made OIFR will allow the Operator to obtain the Niche RMS nominal number relating to this image and submit this for a 'person check' as currently detailed within the iPatrol Standard Operating Procedures and related DPIA.

OIFR Standard Operating Procedures (SOP's) provide a detailed overview of the mechanics of OIFR.



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?

Retention and Erasure

Particular to OIFR and FRT System

- Image of the Subject as captured by OIFR (Probe Image) - immediately deleted in the OIFR Device and FRT system.
- Biometric Template of Probe Image - immediately deleted in the FRT System
- Candidate images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS

Electronic Pocket Notebook

- Electronic Pocket Notebook – MOPI retention of personal information (detailed within ePNB DPIA), not including the Probe Image.

Source System – Custody Images and Missing Person Images

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

Currently there are circa 760k images in the SWP /GWP Niche RMS source system, all images will be bulk uploaded to the Image Reference Database upon pilot go-live with

additional custody images added from the source system ten minutes after image capture in the source system.

Missing person images are updated in the Image Reference Database every hour. This will involve both new images being added and any images which are no longer flagged as missing persons in the source system are also un-enrolled from the Image Reference Database.

The geographical area is limited to the South Wales and Gwent region.

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

Initial deployment of this tactic will be an overt process supported by a communications strategy. Privacy notices have already been amended and distributed as well as being located on the SWP/GWP website.

Operators will provide the Subject with an oral explanation as to rationale and grounds for using OIFR at the location, unless the Subject is unconscious or deceased, in addition to published information accessible to the public.

The Operator will explain that the Subject's Probe Image will be immediately and automatically deleted and not shared with any third party.

The use of OIFR may provide the Operator with additional information and intelligence in order to further utilise other policing tactics such as a power to search or arrest a Subject.

The Subject shall be directed towards the SWP/GWP FRT website for details of the full privacy policy.

When OIFR is utilised the Operator must ensure they do so lawfully, and in an appropriate and proportionate manner. Operators must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject to OIFR, should be supplied with an OIFR information leaflet.

The SWP/GWP Privacy Notice has also been amended to include information on biometric data being processed and signposts the FRT website.

Image Reference Database(s)

Those included in the Image Reference Database 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 Senior Responsible Officer must be satisfied by the steps taken to ensure the composition of the Image Reference Database(s) are not excessive and only includes those who need to be identified by SWP/GWP using OIFR on a strict necessity basis.

Children/Vulnerable Groups
It is possible that there will be processing of children or vulnerable groups however after their Biometric Template generates the return of the similar Candidate Images no other details will be processed and this information will be deleted immediately. The Operator will receive the six similar Candidate Images and further manual checks will be carried out to identify whether that person is on the Image Reference Database(s). There is no automated decision making in the process.

Issues of concern
Proportionality and lawfulness – there are concerns that use of OIFR 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. OIFR will not 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 OIFR.

Function creep – there are concerns that OIFR will be used to monitor movements and action of the public beyond the scope of targeted use or be used for covert surveillance.

Retention – there are concerns that all data captured during OIFR use will be kept as intelligence. There are also concerns that returned Candidate Images 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 of live facial recognition which could be relevant in part to the use of OIFR.

Bias – there are concerns that the software algorithm may contain inherent bias with regard to the protected characteristics of race and sex. The human failsafe of an Operator checking the six similar Candidate Images is not sufficient to meet the Public Sector Equality Duty.

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?

OIFR will enable the Operator to assist with the identification of a Subject. In line with the National Decision-Making Model (NDM) when OIFR has assisted identify a Subject this will allow the Operator to gather further information and intelligence of the Subject, which is recorded on police indices, this will include any risks posed by the Subject often referred to as 'warning markers'. The Operator will then be better placed to assess the threat and risk posed by the Subject and identify an appropriate means of disposal having considered relevant powers and polices. This may include the power of arrest should the necessity test for arrest be realised.

OIFR is policing tactic which is to be used to compliment current policing tactics and will assist with the information and intelligence gathering stage of the NDM. Use of OIFR may at times provide Operators with additional Information and Intelligence which assists with the justification for another policing tactic, to include a power of search and/or a power of arrest.

National Decision-Making Model – UK police

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 SWP/GWP 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 – Liaison and assistance on completion of the DPIA as well as the additionality associated with the formal academic study over the implementation of the technology. 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*. In 2019 the ICO commissioned a report on use of LFR for law enforcement purposes in which the following public opinions were obtained:

- 82% of those surveyed indicated that it was acceptable for the police to use LFR;
- 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;
- 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime; and
- 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.

The public's support holds up even if they were to be stopped by the police as a result of LFR matching them (erroneously) to a subject of interest. 58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.

2. 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.

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

4. SWP Independent Ethics Committee – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.

5. 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.

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

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

8. The Surveillance Camera Commissioner – Professional discussion over project proposals and implementation. The SCC Code pf 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.

9. The Biometrics Commissioner – Professional discussion over project proposals and implementation

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

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

12.The University Police Science Institute – 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 October 2018.

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".

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
Legal power to carry out processing e.g. statute, common law, court order etc. *(please provide details)*	Common law – policing purpose and law enforcement purpose. Police and Criminal Evidence Act 1984 The OIFR Policy provides detailed analysis relating to article 8 of the Human Rights Act and other relevant legal considerations. The collection of an image will engage the right to privacy under Article 8. This is qualified right SWP/GWP must ensure that there is a defined legitimate aim and that interference with this right is justified (as set out above). The actions are proportionate and reduce the potential for further interference with the individual which may be necessary under current practices where the Subject refuses to provide details to an Operator. A Probe Image of the Subject is captured and therefore their personal information will be processed. A Biometric Template of the Probe Image will be created and compared against the existing Biometric Templates of Persons of Interest within the Image Reference Database(s). The practical processing of the Subject will take less than three hundredths of a second. The Subject will not be requested to provide their age, gender and ethnicity as this will be officer defined.

	There will be further processing of the data of Person if Interest located in the Image Reference Databases which is considered necessary in the public interest. Whilst the Biometric Templates already exist the Probe Image will be compared (and therefore processed) against every Candidate image in the Image Reference Databases. The tangible impact of this processing on individuals in the Image Reference Databases will be minimal and consistent with traditional practices where an individual's personal information resides within a policing database. Privacy is engaged, but the justified, proportionate, legal, auditable and necessary intrusion is permitted in relation to the investigation of offences, the prevention of crime and the investigations into missing person and safeguarding enquiries. When an Operator utilises OIFR this will be supported by the use of Body Worn Video which will also be processing personal information and will be detailed in a separate DPIA. The Body Worn Video policy has been amended to mandate that when OIFR is utilised the Operator must record the encounter on their Body Worn Video device. OIFR will assist in reducing the number of persons incorrectly arrested and detained at a police station where their identity cannot be established prior to DNA or fingerprints being obtained. In relation to deceased Subjects, OIFR will assist in identifying and reducing the number of occasions on which a potential next of kin is incorrectly sought to identify a Subject. Current research would suggest that significant criminal offending in South Wales is local and repeat and so comparing potential Subject images against SWP/GWP custody database is considered a relevant tactic when trying to identify a Subject.

<table>
<tr>
<td rowspan="2">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

X Consent
☐ Contract
☐ Vital Interests
☐ Legal Obligation
X Public Task
☐ Legitimate Interests

To note consent and explicit consent are relied upon only for testing purposes.</td>
<td>General: Special category data

X 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</td>
</tr>
<tr>
<td>Law Enforcement: Personal data

X Consent
X Processing is necessary for the performance of a task carried out for that purpose by a competent authority.</td>
<td>Law Enforcement: Sensitive processing

X Consent
X Processing is strictly necessary for the law enforcement purpose; and
X Statutory etc purposes
X Protecting vital interests</td>
</tr>
</table>

	As above consent and explicit consent are only relied upon for the purposes of testing	**X Safeguarding of children and individuals at risk** ☐ Personal data already in the public domain ☐ Legal claims ☐ Judicial Acts ☐ Archiving
Data Protection Act 2018 (to be completed where special category data (part 2) or sensitive processing (Part 3) is being carried out	The primary purpose for processing is for law enforcement as detailed within Part 3 of the DPA. These will include: - Prevention, investigation, detection or prosecution of criminal offences and the prevention of threats to public security. Biometric data such as facial images is sensitive data and so subject to particular conditions. More detailed considerations of the conditions for processing are set out earlier in this document. In summary the main conditions relied upon for sensitive processing of personal data include: - • Statutory purposes. • Administration of justice. • Safeguarding of children and of individuals of risk. • Preventing fraud • Substantial public interest It is considered that the identified processing of sensitive information is strictly necessary for law enforcement purposes and there is a pressing public interest in the outcomes from using this technology which cannot reasonably be achieved through less intrusive means. In order to best serve the public and in particular victims, realising swift and	

	effective justice is a considerable aim. It would be almost impossible for any one police officer to be able to identify effectively an individual from potentially thousands of individuals from their face alone; use of OIFR assists the front-line officer identify, help or dismiss a Subject. A similar aim could be achieved by providing the officer with a printout of persons in the Image Reference Databases but this would present greater Data Protection concerns in addition to the practical difficulties with providing an up–to- date, accurate and auditable list. It is believed that the use of OIFR will be far less intrusive in identifying a Subject than employing other methods, such as repeatedly checking a false name(s) provided by the Subject against police indices and bringing an individual into custody unnecessarily. Data may also be processed under the GDPR, for example for missing persons; the relevant conditions in this regard include: - Article 9(2)(c) – vital interests Article 9(2)(a) – explicit consent In circumstances where we seek consent, we will make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the relevant condition. Article 9(2)(g) Substantial Public Interest Article 9(2)(j) – Historical research or statistical purposes As with the law enforcement purposes the conditions are set out in more detail earlier in this document.

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.	Initial deployment of this tactic will be an overt process supported by a communications strategy. Privacy notices have already been amended and distributed as well as being located on the SWP/GWP website. Operators will provide the Subject with an oral explanation as to rationale and grounds for using OIFR at the location, unless the Subject is unconscious or deceased, in addition to published information accessible to the public. The Operator will explain that the Subject's Probe Image will be immediately and automatically deleted and not shared with any third party. Information regarding ethnicity and gender can be added in by the Operator as an additional safeguard to reduce the likelihood of error in the comparison process. Information added to the ePND by the Operator will retained in the usual way according to MOPI. The Subject shall be directed towards the SWP/GWP FRT website for details of the full privacy policy. The SWP/GWP Privacy Notice has also been amended to include information on biometric data being processed and signposts the FRT website. 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)*	The Subject shall be directed towards the SWP/GWP FRT website for details of the full privacy policy. The SWP/GWP Privacy Notice has also been amended to include information on biometric data being processed and signposts the FRT website. Subject Access – members of the public would be able to exercise this right as the force would be able to locate their data retrospectively as a record of OIFR enquiry is inputted into the Operator's ePNB. OIFR use is auditable via the Operator's ePNB. OIFR transactions are uniquely coded and can be searched to provide details that would assist a subject access request. Right to rectification – Subjects will be able to challenge the processing where a match has been identified by OIFR and the Operator. Right to erasure – The information is generally deleted as set out above. If for any reason information is retain this right will only apply where appropriate Right to data portability – not applicable Right to object – Each use of OIFR 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. All decisions will have manual intervention.
How will you ensure that the data being processed is accurate and up-to-date? Will the processing allow you to erase or rectify inaccurate data without delay?	Members of the public – processing will be near real time. Initial user validation in a non-live environment has been conducted. In excess of 200 controlled searches have been carried out. On all occasions when the Probe Image is of a Subject that exists in the Image Reference Databases the correct Candidate Image is returned to the Operator (placed number one of the six Candidate Images returned.)

	The validation process focuses on any potential age, gender and ethnic imbalance. These concerns have been mitigated during the validation period with further focus anticipated during the pilot period and independent academic evaluation. There will also be manual consideration of Possible Matches by an Operator prior to any action being taken. 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. The SWP/GWP supplier has also been held in high regard by the NIST in its 2019 evaluation of over 200 algorithms. Data will be checked against source SWP/GWP databases, managed in accordance with MOPI standards. These databases are kept up to date as required for effective law enforcement so that personal data which is known to be inaccurate, materially incomplete or no longer up to date is not transmitted. The core source database is Niche RMS which undergoes rigorous checks and balances to ensure the data is accurate and fit for purpose. Niche RMS makes clear distinctions between different categories of subject (e.g. suspects, persons convicted, victims, witnesses) and this information will be transferred to the OIFR Device upon use of OIFR.

	In relation to data obtained from the Subject, this will consist of an image of their face. Operators are provided with a 'top five' good practice guide via the OIFR Device prior to image capture to ensure the best possible image is captured for accuracy, avoiding capturing other individuals in the image. SWP/GWP personnel will take all reasonable steps to ensure that each image on a Image Reference Database does actually pertain to the intended person. No action will be taken against a Subject without human consideration of a Possible Match. OIFR is integrated into the existing iPatrol mobile application which has been in existence since 2015. iPatrol is a joint venture between SWP/GWP and a software company in which SWP/GWP have played a pivotal part in its development. iPatrol is accessible to SWP/GWP officers since 2015 via their mobile phone and acts as the gateway into existing police indices, to include Niche RMS, the Warrants database and the Police National Computer. SWP/GWP continue to act as the primary forces for the development of iPatrol which is coordinated through the internal Digital Services Division (DSD.) Data that is recorded in Operator ePNB cannot be deleted by the Operator but a detailed amendment can be made.
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 OIFR use 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/GWP's complaints / conduct investigation policies.

	Technical systems and standard operating procedures help ensure that data is properly retained or deleted. Processing mechanisms, OIFR Policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes. The Operator defines the Subject's age, gender and ethnicity whenever OIFR is utilised regardless of whether a match is made. The Operator defined details will be consistent with the current stop/search protocols. The primary requirements for this are for audibility purposes and to assist in any future FOI requests. There is likely to be significant public interest in the results of the trial. OIFR has been designed to service these requests and to provide accountability. These details are not required to assist in the identification of the Subject. The Candidate Images on the Image Reference Databases 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?	**Particular to OIFR and FRT System** • Image of the Subject as captured by OIFR (Probe Image) - immediately deleted in the OIFR Device and FRT System. • Biometric Template of Probe Image - immediately deleted in the FRT System • Candidate images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS **Electronic Pocket Notebook**

	• Electronic Pocket Notebook – MOPI retention of personal information (detailed within ePNB DPIA), not including the Probe image. **Source System – Custody Images and Missing Person Images** Please refer to Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4) as the recommended periods apply to the following categories of data: 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 then review Group 2 – 10-year clear period then review Group 3 – 6-year clear period Group 4 (missing persons) – 6 years then review
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	Identified privacy risks are set out in this document but primarily involve the processing of facial imagery from which biometric data is extracted (sensitive data). Mitigation of risk from the outset was secured by the provision of a force hosted FRT System. The Image Reference Database of custody images are restricted to the SWP/GWP force

their ongoing ability to keep the data secure?	area custody database. The Image Reference Database of missing persons are also restricted to missing persons from within SWP force area. Operators are appropriately vetted. Sharing with third parties such as independent academic bodies in the provision of academic review (where individuals are also vetted) occur through an Information Sharing Agreement (ISA). Data transfer issues have been addressed in this document and retention will be compliant with MOPI requirements. Training and Standard Operating Procedures will be provided to all Operators utilising OIFR. Retention periods are set. The processing is auditable to identify misuse. Devices are police issue therefore have appropriate security measures including authentication and time outs. No action is taken without manual consideration of the Candidate Images by an Operator. The application will be password encrypted. Each user of the application has to authenticate into iPatrol via username and password (active directory). The transmission of images and other personal information from the Operator's

	smart phone to on premise servers is undertaken via a Virtual Private Network. The transmission of personal information from officer smart phone to on premise servers has been in place since 2015 and is detailed in the iPatrol DPIA. The use of FRT is governed by a number of codes of practice including those applying to the police such as PACE. Internal governance arrangements have been established for OIFR with governance and accountability provided by the Facial Recognition Technology and Biometric Board. Onward accountability is provided by the allocation of a Senior Responsible Officer (SRO). The data is held securely on SWP/GWP systems accessible to SWP/GWP officers and staff which is fundamentally permission based. Officers leaving SWP/GWP automatically have their account disabled and therefore would no longer have access to the information. The data held on SWP/GWP systems is not specific to OIFR (it provides OIFR with the information needed to compile and generate Image Reference Database(s) and relates to policing information generated following the use of OIFR). When a Candidate Image is returned during the use of OIFR there is Operator intervention to assess the images and where necessary the Subject identified as a Possible Match will be engaged by an officer before any further action is taken. The use of OIFR as a tool to identify individuals of interest to SWP/GWP 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/GWP OIFR Documents provide for the training of officers and staff involved in the use of OIFR to be principally delivered by a DSD trainer. The training helps ensure role specific: 1. familiarity with SWP/GWP OIFR Documents; 2. knowledge of grounds and reason for OIFR use; 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 Possible Matches; 6. knowledge of how to configure OIFR to maximise system performance, and how to minimise impact on others; 7. understanding of the characteristics of OIFR that affect the likelihood that a Possible Match is reliable. Police officers and Police Community Support Officers have the same level of access to iPatrol and OIFR. Delivery of OIFR is restricted to sixty pilot officers via Airwatch which is the secure application utilised to manage SWP/GWP mobile phone assets. Access to the FRT System and supporting source databases utilises roles to assign privileges. This means that individuals can be assigned levels of access based on a permission level, the higher the permission level will allow the individual greater access to change application settings.

	All use of OIFR will be recorded in the Operator's ePNB. Any breach of this database would be reported to the Information Management team via an online form that can be found on the SWP/GWP intranet site (BOB/BEAT.) Instructions of when and how to complete this form are detailed on the SWP/GWP intranet site. Any lost devices are protected by multi-layered password protection and can be wiped remotely. Liaison continues also with the SWP/GWP Force Information Security Officer, Senior Information Risk Owner and Information Commissioner's Office.
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. Data used for this process will be held on SWP/GWP premises based in the UK
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. Information could be shared with Home Office Biometrics, the Defence Science and Technology Laboratory and academic partners as part of the wider academic evaluation over the proof-of-concept matters within the project. However, this could only be facilitated using available information captured within the defined retention periods.

	In technical terms, data is never transferred to academic partners as the data is placed into a 'viewing pot'. The audit functionality adds an additional layer of protection of the data. An information sharing agreement will exist between SWP/GWP and academic evaluators in relation to the academic research. The information we are sharing with academic partners would include access to the ePNB audit logs. We will also provide academic evaluators with the wider details of OIFR use to include Image Reference Database rationale and size. Full Image Reference Database content will not be shared with academic evaluators. Operating staff and academic evaluators will all be vetted and cleared to at least MV/SC level. Details of the pilot will also be shared with active members that currently make up the National Biometric Strategy Board and NPCC Facial Recognition Technology Board. Membership of these boards includes interested regulators and commissioners, to include the Biometrics Commissioner, Information Commissioner, Surveillance Camera Commissioner, Forensic Science Regulator and the National Police Chief Scientific Adviser.

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	There is a risk with the immediate with the immediate deletion of the Probe Image when an individual is subject to OIFR and they are not identified. The Operator only records basic information about the Subject it may at times prove difficult to identify the query should a Subject later make a subject access request.	M	M	M
2	As a result of OIFR use 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
3	As a result of OIFR use there is a risk that it may 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
4	An individual may wish to complain about OIFR use as during the trial this will be limited to officers and location.	M	M	M
5	OIFR is used which is part of an incorrect identification which subsequently involves a Subject's liberty being revoked and an unlawful arrest.	L	H	H
6	As a result of the wide-ranging capability of OIFR to process biometric data there is a risk that the processing of personal data may be excessive resulting in regulatory action.	M	H	H
7	As a result of the capability of OIFR to process high volumes of data there is a risk that it may be deployed for 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
8	Image Reference Databases will not be live data and therefore vulnerable individuals may	L	L	L

	be failed to be identified potentially leading to increased harm.			
9	As a result of potential incomplete deletion exercises there is a risk that Image Reference Databases 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 intervention and potentially cause unwarranted and unjustified damage and distress to individuals	M	H	H
10	As a result of different scenarios in which a person may be reported as missing there is a risk that the use of OIFR to identify 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
11	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
12	As a result of inconsistent guidance around the use of OIFR there is a risk that officers may exercise too much discretion around the selection of the Image Reference Database resulting in excessive and unlawful processing of data which may lead to legal challenge, complaints and potential enforcement action.	H	H	H
13	There is a risk that officers involved in the use of OIFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the use of OIFR and potential breaches of the DPA'18 which may result in enforcement action, legal action and financial penalties.	M	H	M
14	As a result of lack of training and awareness there is a risk the data entered onto the Image Reference Databases is not treated within the correct Government Protective Marking Scheme (GPMS) resulting in	L	L	L

	adequate protection when handled and potential loss and damage			
15	As a result of lack of training and awareness there is a risk that the Images Refence Databases or other data generated by OIFR is unlawfully disclosed to third parties	L	M	M
16	As a result of technical failure there is a risk that the equipment will not function correctly resulting in incorrect returns or failure to identify Possible Matches resulting in potential damage and distress or threat risk and harm to others	L	H	M
17	If multiple individuals are captured in the Probe Image there is a risk their personal information will be processed during the image capture.	L	M	M
18	The processing of personal information of children and vulnerable persons in the absence of parent or guardian which may lead to distress for the individual.	M	M	M
19	The use of OIFR may lead the general public to perceive that OIFR is being used disproportionality towards persons from ethnic backgrounds which may lead to legal challenge, complaints and potential enforcement action.	M	H	H

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	To mitigate this the GPS location of the enquiry is recorded in the Operators ePNB and also the date and time. There will also be an interaction between the Subject and Operator so it is extremely likely they will be aware that they have been subjected to OIFR.	Reduced	L	Y

2	A communications strategy will be in place prior to OIFR pilot to ensure that all available means of communicating the fact that the pilot is taking place via various channels including digital and physical, and information is available to the public to ensure they can be confident that the decisions made to pilot are based on firm evidence and transparent analysis.	Reduced	L	Y
3	The assessment prior to any use of OIFR 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 during use.	Reduced	L	Y
4	To date there has been no official complaint about SWP use of Facial Recognition technology however there has been an individual who may have been subject to Live Facial Recognition who brought a Judicial Review heard in May 2019 with subsequent Appeal in June 2020. Operators are encouraged to obtain and record details of all Subjects.	Reduced	L	Y
5	Failure to allow an Operator to capture an image does not constitute a criminal offence and an arrest may not be made. If the Probe Image is incorrectly matched against a Candidate Image this may result in an unlawful arrest. The risk here is no more prevalent than in current police practices when integrating police indices.	Reduced	L	Y
6	The Operator assessments prior to use of OIFR will consider and document why less intrusive methods are not appropriate and justifying the use of OIFR based on information and available at that time.	Reduced	L	Y
7	Any covert surveillance will require authority under the Regulation of Investigatory Powers Act 2000 as per arrangements for any covert surveillance.	Eliminated	L	Y
8	The latency between Image Reference Databases and source systems has been reduced to ten minutes which will significantly reduce the opportunity for missed images visible during use of OIFR.	Reduced	L	Y

9	Image Reference Databases 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 interventions will be made without checks being made on Possible Matches without manual intervention to reduce any damage and distress. SWP/GWP are actively engaged with the Niche RMS supplier to develop automated deletion of non-convicted custody images. They are also an active participant of the NPCC Records Management working which have been set up to lead on a national solution. SWP/GWP have also advertised within all custody suites the process for non-convicted image deletion requests.	Reduced	L	Y
10	Where OIFR is being used to identify 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. .	Reduced	L	Y
11	The force will have in place appropriate policy documents for OIFR for processing under Part 2 and Part 3 of the Data Protection Act 2018	Eliminated	L	Y
12	OIFR SOPS stipulate grounds and reason for use of OIFR ensuring consistency and oversight for each use.	Reduced	L	Y
13	As part of OIFR training appropriate data protection training will be provided.	Reduced	L	Y
14	All SWP/GWP staff/ officers are trained in respect of the GPMS. Image Reference Databases are automatically complied in a secure environment to which the public do not have access. All Image Reference Databases are appropriately stored prior to the OIFR pilot.	Accepted	L	Y
15	Officers/Staff involved in the pilot do not have ready access to the complete Image Reference Databases and are briefed in respect of Image Reference Database	Reduced	L	Y

	image circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, pilot officers and technical support staff. Any action following use of OIFR may involve SWP/GWP working with other police forces, law enforcement bodies and other agencies to assist SWP/GWP in discharging its common law policing powers. This action will not require the sharing of biometric data but may require SWP/GWP to share personal data, as it would for any investigation, in accordance with SWP/GWP's routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect OIFR.			
16	The technology has been trialled and tested by SWP. NEC algorithms have also been evaluated by NIST and the Department of Homeland Security and SWP/GWP pays regard to these findings. All relevant information is logged for audit purposes. SWP/GWP OIFR Documents also outline points relating to OIFR to ensure that it is used in a way that maximises its effectiveness. The ongoing effectiveness of SWP/GWP's use of OIFR during the pilot will be reviewed by the FRT and Biometrics Board and the SRO. This will help ensure that any future OIFR use will reflect learning identified from the pilot and that the use of OIFR remains an effective and proportionate policing tool	Reduced	L	Y
17	During use of OIFR and prior to capturing a suitable Probe Image the Operators receive a screen prompt to ensure that only one Subject to be captured in the Probe Image.	Reduced	L	Y

18	One of the primary functions of OIFR is to protect persons who are vulnerable and it is likely that OIFR will be utilised on children and vulnerable persons. This will be carried out at times in the absence of a parent or guardian in a similar manner to the way which Body Worn Video or a name check of that Subject is currently undertaken.	Accepted	M	Y
19	During use of OIFR the Operator will have to record the officer defined ethnicity of the Subject as well as details of other protected characteristics. This will allow SWP/GWP to be able to monitor and respond to any FOI requests relating to disproportionate use.	Reduced	L	Y

Step 7: Sign off and record outcomes

Action	Name, position, date	Notes
Measures approved by:	Chief Inspector Scott Lloyd 22.10.2021	Actions must be integrated back into the project plan with completion dates and action owners
Residual Risks approved by	Chief Inspector Scott Lloyd 22.10.2021	If accepting residual high risks, refer to DPO to consider ICO consultation before proceeding
DPO advice provided	Louise Voisey 25.10.2021	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 OIFR by SWP/GWP, 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/GWP utilise OIFR 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 25.01.2022	If overruled, an explanation must be provided.
Comments:		
Consultation responses reviewed by:	Chief Inspector Scott Lloyd 16.11.2021	If the decision does not align with the views of the consultees please explain
Comments:		
This DPIA will be kept under review by:	Inspector Andrew Hedley, Operational FRT lead	The DPO should also review ongoing compliance with DPIA.

Annex A – Information Available to the Public

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

A key measure is the publication of SWP/GWP's Privacy Notice, SWP/GWP policy on protecting special category and criminal convictions, and key SWP/GWP OIFR Documents on the SWP/GWP website. Whilst SWP/GWP 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 subject to OIFR and those who may be placed on Image Reference Database to understand the standards SWP/GWP, as a public body, operates to. In doing so, SWP/GWP provides details about the requirements to use OIFR, and the considerations and constraints relevant as to who may be placed on a Image Reference Database. In this way, SWP/GWP's use of OIFR 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/GWP Privacy Notice:	• Data Controller identity and contact details • Data Protection Officer details • The scope and purposes for processing personal data by SWP/GWP • 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/GWP policy on protecting special category and criminal convictions	• SWP/GWP 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/GWP OIFR Legal Mandate	• The lawful basis for processing data in relation to OIFR. 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 Freedom of Information Act 2000
SWP/GWP OIFR Policy Document	• An outline, strategic intent and objectives for the use of OIFR and how personal data will be used by the FRT system • Data retention periods applicable to OIFR
SWP/GWP OIFR Standard Operating Procedure Processes	• Outlines measures relevant to considering when the OIFR can be used by SWP/GWP. • Image Reference Database considerations including the basis on which images may be added to an Image Reference Database and considerations relevant to the sources of non-police originated imagery.
SWP/GWP OIFR 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/GWP OIFR 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/GWP complies with the Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of personal data.
SWP/GWP OIFR Equality Impact Assessment	• Promotes all aspects of equality. • Ensures compliance with the law, taking into account of equality and human rights.