Joint Data Protection Impact Assessment (DPIA) and Information Security Impact Assessment

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	SWP/GWP	
Subject/Title of DPIA	Operator Initiated Facial Recognition	
Name of DPIA adviser	Louise Voisey	
Force Information Security Advisor	Lee Bowen	
Key dates	Started	
	Completed	19/11/2024
	Review	

Project Name	OIFR
Responsible Owner	Phil Oseng-Rees
Business Area/Department	Digital Services Division
Proposed implementation date	14/12/2024
Reference No. *(to be allocated by IG)*	DPIA256

It is recommended that you refer to the DPIA guidance and process documents (hyperlink) to assist in the completion of these sections. Where External Cloud based suppliers are being used please complete Annex A.

Risk matrices are at Annex B

Step 1: Project Aims and Processing

Identify why the processing requires a DPIA *(indicate which applies with an 'x')*

x	Type of processing	Brief details
	Systematic and extensive profiling	
	Public Monitoring	
	Denial of Service	
x	Data Matching	Biometric templates are matched
	Tracking	
	Risk of Harm	
	Automated Decision Making	
	Large scale use of sensitive data	
x	Innovative technology	Biometric matching for the purpose of uniquely identifying an individual
x	Biometrics	Facial recognition
x	Invisible processing	Facial recognition; biometric matching
	Targeting children/vulnerable adults	
x	Special category/criminal offence data	Biometric data; custody images
	Other	

Suppliers or sub-contractors		
Company details	Name	NEC
	Trading name if different	NeoFace
	Address	
	Main establishment if not in the UK	
	Companies House Number	
Point of contact	Name	
	Role	
	E-mail	
	Tel. No.	
Data Centres	Location (s)	
	On prem	
	Cloud	
Back ups	Location (s)	
	On prem	
	Cloud	
Location of Support and Maintenance		
Procurement stage		

Aims and Objectives
Describe the context, purpose and aims of what the processing is intended to do.

Aim

There are increasing demands on policing – financially, resource and high workloads. Great emphasis has been placed on a data driven and preventative approach whilst harnessing new technology and forensics to rebuild public trust. The government has indicated that outdated processes and systems have left the police struggling to keep up with a fast-changing criminal landscape.[1] The Science and Technology in Policing strategy and the National Policing Digital Strategy states that "Central to our objective are plans to modernise core digital systems, putting the power of data and information in the hands of our staff".[2] The National Policing Digital Strategy[3] is clear that increasing officers' operational efficiency is a priority and that a dynamic workforce will be digitally enabled by default, by unlocking value from data, whilst maintaining public trust. This includes ensuring security, ethical and responsible use of data and utilising analytics to extract insights to deliver better outcomes. Technology such as Facial Recognition Technology (FRT) can help the police quickly and accurately identify those wanted for serious crimes, as well as missing or vulnerable people. It also frees up police time and resources, meaning more officers can be out on the beat, engaging with communities and carrying out complex investigations.

The aim of Operator Facial Recognition (OIFR) is to run a pilot for 12 months which facilitates utilisation of biometric data matching to identify subjects who are engaged by officers for a legitimate policing purpose and are either unable or unwilling to identify themselves, against the police custody database or missing persons database. At the end of the pilot, a review will take place to determine whether to continue to use OIFR as business as usual.

The use of OIFR involves the processing of personal data and therefore data protection law applies, whether it is for a trial or routine operational deployment.

The processing of personal data by 'competent authorities' (s.30 Data Protection Act 2018 (DPA)[4]) for 'law enforcement purposes' (s.31 DPA 2018[5]) is covered by Part 3 of the DPA 2018. To note that not all policing purposes fall within the definition of law enforcement purposes e.g. missing persons where there is no suspicion of criminal activity. In such cases, Part 2 DPA will apply.

[1] Home Office on Police Reforms November 2024
[2] S&T in the NPCC's strategy
[3] National-Policing-Digital-Strategy-2020-2030.pdf
[4] Data Protection Act 2018
[5] Data Protection Act 2018

Specifically, the use of OIFR for law enforcement purposes constitutes 'sensitive processing' (s.35(8)(b) DPA 2018[6]) as it involves the processing of biometric data for the purpose of uniquely identifying an individual. Such sensitive processing relates to facial images captured and analysed by the software; and must pay particular attention to the requirements of s.35, s.42[7] and s.64 DPA 2018[8].

Sensitive processing occurs irrespective of whether that image yields a match to a person on an Image Reference Database, or the biometric data of unmatched persons is subsequently deleted within a short space of time.

Data protection law applies to the whole process of OIFR, from consideration about the necessity and proportionality of using it, the compilation of Image Reference Database, the processing of the biometric data through to the retention and deletion of that data.

Part 1: Use of OIFR

Context

Policing now deals with an ever more transient population, with criminals crossing force borders in order to commit offences and drawing on vulnerable people as victims of crime and also criminal exploitation. Given this ability to move freely, the efficacy of the 'local Officer' to know everyone in their area by sight and name and be able to make informed decisions based on information known to them is limited at best.

It is an expectation that the police will engage with the public and communities in the course of their duties and in the majority of these cases, identification of that individual will not be required.

In circumstances where the Officer has a policing purpose, the Officer may require the Subject to provide their name and address in order that further checks can be undertaken. This can lead to problems where a Subject may refuse to provide their details, provide false details or be unable to communicate their details to the Officer. This can lead to further intrusive police activities such as arrest, where the necessity is to confirm name and address, being required where, if that information were available at the point of initial interaction, the Officer could make an informed decision on appropriate action to take based on up-to-date information and the arrest may no longer be the proportionate outcome.

[6] Data Protection Act 2018
[7] Data Protection Act 2018
[8] Data Protection Act 2018

Detention of the Subject due to refusal to provide identification details may lead to them spending extended periods of time in custody whereas more appropriate and proportionate outcome may be available. This would also reduce the resource impact on frontline policing, increasing numbers of Officers able to respond to the needs of the community.

Where a Subject provides false details, this could lead to delays in time critical enquiries in investigations which could result in the loss of evidence or investigative opportunities, and potentially imposition of bail conditions where the delay has caused enquiries to remain outstanding that would allow a matter to progress to the point of a full code charging decision. Bail conditions can have significant impact on the life of the Subject and all reasonable opportunities to reduce the time spent on bail should be taken.

In circumstances of persons unable to provide their details, this could relate to vulnerable persons or persons in mental health or medical crisis. The delay in identifying these persons could be life changing, even resulting in death, if prompt action is not taken to ensure their safeguarding.

The delay in identifying a deceased person can lead to time delays for the next of kin being notified and may have a negative impact on the ability of the investigating officer to identify and set Golden Hour lines of enquiry when investigating sudden, unexpected deaths and / or murders.

OIFR will not be used in lieu of traditional police methods of identification and will only be used following an engagement or attempted engagement between an officer ('Operator') and the person who has been stopped ('Subject'). The Officer should exhaust all reasonable, less intrusive opportunities to identify the Subject before using OIFR. The image capture function only focuses on the subject, with the operator being able to crop the subjects face before submitting it for facial marching, removing the risk of inadvertent capture of images of any other members of the public who are in the surrounding area at that time, preventing any unintended processing.

Necessity

s.35(5) DPA 2018 requires that where sensitive processing is taking place for a law enforcement purpose without consent it must be:

- Strictly necessary for a law enforcement purpose;
- Meet one of the conditions set out in Schedule 8 DPA 2018[9]; and
- An appropriate policy document must be in place

The public expects the highest standards of compliance by the police and other law enforcement authorities when processing sensitive data. In the ICO's Opinion on Use of Live Facial Recognition in public spaces 'strictly necessary' is described as "'a high bar, but it must be reached before the

[9] Data Protection Act 2018

sensitive processing can take place under Part 3 DPA 2018, i.e. the processing must be more than merely 'necessary' for the law enforcement purpose and cannot be reasonably achieved by a less intrusive method. This recognises that:

- sensitive processing, in this case of biometric data for the purpose of uniquely identifying an individual, is taking place;
- this gives rise to higher risks to individuals' rights; and
- the processing therefore requires higher levels of protections and safeguards.

Purpose

The purpose of the processing is to support existing police powers to identify a subject, such as making a direct request face to face, which then enables the officer to check the subject's details against police records to verify that information. Where the traditional method of identification fails, OIFR will be used to:

a) Support the identification and arrest of people wanted for criminal offences;
b) Support 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, sex offenders etc);
c) Support the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed.
d) Support the identification of deceased persons, to assist the coroner.

This will result in increased effectiveness in protecting the public and vulnerable subjects from immediate risk of threat and harm, reducing the impact on the wider public when dealing with subjects who are matched to the police record by containing potential threats or identifying specific warning markers[10], and allocating police resource and demand in the most effective way and providing a better public service. Ordinarily where the subject's identity cannot be established due to refusal or an inability to respond that individual may be taken into custody and police will then need to access multiple nominal records in order to find the correct one.

Requirements for use of OIFR

Use of OIFR must meet at least one **ground** and one **reason** set out below. (The powers of the police to stop individuals is not within the scope of this DPIA).

[10] These may have been placed on the record to indicate that an individual is violent or suffers from certain conditions enabling officers to respond accordingly.

Grounds

For OIFR to be used, the identity of the Subject must be unknown and reasonable, less intrusive enquiries to identify the Subject must have been exhausted. There must be at least one of the following grounds present:

The Subject Is suspected:

a. To have committed or be in the process of committing a criminal offence or is unlawfully at large/ wanted on warrant or recall to prison with further police action required[1].

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

c. To be a missing persons deemed increased risk[2].

d. There is an immediate threat to life or immediate risk of serious harm[3] - including safeguarding the welfare of vulnerable people, including children at IMMINENT risk of abuse or otherwise harmed.

e. To be deceased or it has been confirmed that they are deceased

Reasons
In addition to the grounds existing, **at least one** of the following reasons must be present:

a. The Subject is unable to provide their details[4]

b. The Subject has refused to provide their details

c. It is reasonable suspected the Subject has provided false details

[1] '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. It will be the responsibility of the Operator to justify any action taken following the use of OIFR.
[2] '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.
[3] 'There is an immediate threat to life or Immediate risk of serious harm - including safeguarding the welfare of vulnerable people, including children at IMMINENT risk of abuse or otherwise harmed'.
This ground will reflect that OIFR is necessary is to manage risk of serious harm or an imminent need to safeguard an individual ensure their continued welfare. The interpretation of this definition will reflect the definitions set out in S.61A(7)(g) Investigatory Powers Act 2016 .'
[4] 'The Subject is unable to provide their details'.
For the purposes of clarity, this reason may include:
Persons who are deceased or suspected deceased, unconscious, incapable through drink or drugs, mental health, unable to communicate due to a language, or age barriers. 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/ translation services) in order to facilitate identification prior to use of OIFR.

Lawfulness of using Facial Recognition for a policing purpose

The lawfulness of using facial recognition (albeit Live Facial Recognition) in policing was considered in the case of *R (Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058*[11] in which the Information Commissioner's Office and the Surveillance Camera Commissioner were Interested parties. This also dealt with considerations in relation to interference with Art 8 ECHR, and the Public Sector Equality Duty in relation to the NeoFace Algorithm. The principles set out in that judgment are applied where relevant to use of OIFR.

The powers of the Police are established in common law. The exercise of these powers should be necessary, proportionate and compatible with human rights[12] and equalities[13] legislation. The misuse of police powers is not normally a criminal offence but is a failure to uphold the policing standards of professional behaviour[14].

[11] Microsoft Word - R (Bridges) -v- CC South Wales _ors Judgment.docx
[12] https://www.legislation.gov.uk/ukpga/1998/42/section/6
[13] https://www.legislation.gov.uk/ukpga/2010/15/section/149
[14] https://www.legislation.gov.uk/uksi/2020/4/schedule/2/made

Article 8 ECHR

SWP/GWP acknowledge that the taking of an individual's image may constitute an interference with their Article 8 Right to a Private Life. The procedures and justification for use of OIFR are designed purposely to ensure that there is a clear and recorded rationale for such interference in accordance with the law.

In *R (on the application of Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058), the Court of Appeal concluded that the Data Protection Act 2018 provided "an important part of the framework in determining whether the interference with the Appellants Article 8 right was in accordance with the law". The application of the Data Protection Act 2018 to OIFR is set out in detail in Step 4 below. In addition, the 4-part test in *Bank Mellat v HM Treasury (No2)[2014] AC700*[15] determines whether an interference with Article 8 is proportionate:

1. Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. Whether it is rationally connected to the objective;
3. Whether a less intrusive measure could have been used without unacceptably compromising the objective; and
4. Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

This document acknowledges that subject's Article 8 rights are engaged and that OIFR may process personal data of individuals not on the Image Reference Database.

In response to the 4-part test referred to above:

Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right	The objective is to identify an individual who has refused or is unable to identify themselves on request, who is suspected of committed or be in the process of committing a criminal offence or is unlawfully at large/ wanted on warrant or recall to prison with further police action required; is subject of bail conditions, court order or other restriction that would be breached if they were at the location at the time is a missing person deemed increased risk; is an immediate threat to life or immediate risk of serious harm, or; is deceased or it has been confirmed that they are deceased.

[15] https://www.judiciary.uk/wp-content/uploads/2019/03/bank-mellat-v-hmt-final150319docx.pdf

	Based on these grounds it is sufficiently important to justify limitation of a fundamental right.
Whether it is rationally connected to the objective	It is imperative for an officer to be able to respond proportionately and promptly, with information to support informed risk assessment and decision making, the outcomes being to apprehend the subject and protect the wider public safety or take appropriate actions to safeguard individuals at risk. Informed decision-making serves to support Operators in justifying intrusive tactical options such as arrest or to negate the necessity to arrest by providing information to the Operator at the point of interaction to support alternative, less intrusive outcomes. Therefore, the outcome must be that it is rationally connected to the objective
Whether a less intrusive measure could have been used without unacceptably compromising the objective	Less intrusive measures are employed as a matter of course i.e. traditional methods of requesting details from the individual under existing police powers. OIFR is intended to be utilised where reasonable less intrusive enquiries have been exhausted and it is necessary to identify the individual for a policing purpose. Where a policing purpose exists, OIFR enables the officer to identify the individual who has refused or is unable to identify themselves in response to a request at the scene, rather than detain the individual in front of others and at their inconvenience. Where there is no match between the biometric template and the Image Reference Database no record of the image of the Subject is retained, with the OIFR app automatically deleting the image with no means of recovery.
Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.	Based on the information above and technical/organisational controls and measures detailed further in this document, there is a fair balance between the rights of the individual and the wider interests of the community. The processing will facilitate police actions which, if done via traditional measures will require more physical intrusion for the individual by way of possible detention, in detail and visible processing of more records and personal information to try to identify and match

	the subject manually whilst raising the potential risk of harm to the public or to the subject as a result of delays in accessing the relevant information in a timely manner.

Taking into consideration to answers to the test above, whilst SWP/ GWP acknowledges that Article 8 is engaged, interference is justified in accordance with the law (i.e. police powers under common law.

OIFR is an overt policing tactic.

OIFR can be used wherever the Operator has lawful access and a policing purpose for use, this will include both public and private places.

OIFR use will be identified as being necessary by the information and intelligence when considering the reason and grounds for use and the case supporting the prospects of identifying the Subject. However, the Operator must also consider the reasonable expectations of privacy the general public may have when in a public and/or private place. Some places, and the people expected to be at some places by their nature, attract greater privacy expectations than others.

Examples of such locations would be:
Hospitals, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), care homes, locations used for assemblies and/or demonstrations.

Whilst these greater expectations of privacy do not preclude the use of OIFR, the Operator should consider all reasonable options to minimise collateral intrusion and mitigate the impact upon the Subject and those who are at the location but are not subject of OIFR. This includes cropping the image taken, which must also meet the image quality requirements built into the app.

<u>Article 11 (Right to protest)</u>
It should be noted that OIFR is not designed to be deployed on a large scale and the reasons and ground for use mean that it can only be used in specific circumstances where officers engage with single individual. OIFR is not designed for the purpose of scanning dense crowds. OIFR is designed for the identification of a single Subject following an engagement or an attempted engagement for a policing purpose. For this reason, it may be deemed unsuitable to use OIFR in densely crowded areas where the risk of collateral intrusion may be unmanageable.

Where OIFR is used at densely crowded locations or locations used for protest/ assembly, it may have an impact upon individuals who are lawfully exercising their human rights under articles: 8 - right to private life, 9 - freedom of thought, belief and religion, 10 - freedom of expression, and 11 - freedom of assembly. Whilst these rights are qualified, this still imposes a duty upon public bodies to ensure that the use of such technologies does

not unnecessarily or disproportionately impact the ability of individuals to exercise these rights. It must be recognised in the Judge's ruling in R v Bridges at Divisional Court whereby the level of intrusion of taking a photograph of an individual caused 'negligible' intrusion and the "any impact that has very little weight cannot become weightier simply because other people were also affected".

Where the decision to utilise OIFR in such circumstances is made, Operators should consider all possible options to minimise collateral intrusion. Consideration should be given as to whether the subject of OIFR can be moved to a more suitable location where other members of the crowd are less likely to be potentially captured as collateral intrusion. The Operator should then take all reasonable steps to use the cropping tool included to further minimise collateral intrusion.

If it is not safe or practicable to move to a more suitable area or the subject is willing to co-operate with the OIFR process but not to move from the location, this engagement will (where possible) be captured on BWV and recorded in the ePNB of the Operator as additional information through the OIFR app.

Figure 1. An example of the information an officer must record when using OIFR

Fairness and Transparency

Operators are reminded of the importance of effective tactical communication prior to and during the use of OIFR, and that any action taken must be considered in line with the National Decision-Making Model[16] and the Code of Ethics[17].

Operators have no powers to use force for the purpose of obtaining a Probe Image for OIFR use.

Wherever reasonably practicable to do so, the Operator will inform the Subject that they intend to use OIFR and the Operator must provide details for the reason(s) and grounds for use. **TO NOTE: Operation of OIFR is not based on consent**

When using the OIFR app, the Operator will be provided with prompts in addition to what they have ingested in specific OIFR training:

- The Operator must record any concerns raised by the Subject relating to the use of OIFR within the circumstances free text field.
- The Operator will inform the Subject that their information will not be shared with any third party and the Probe Image and Biometric Template
- created from that Probe Image will be automatically and immediately be deleted.
- The Operator will utilise the below mnemonic to assist them when interacting with the Subject prior to obtaining the Probe Image:

  Reason for use

  Officer's details

  Grounds for use

  Explain that the image will not be saved, and further information can be found on SWP/GWP FRT website

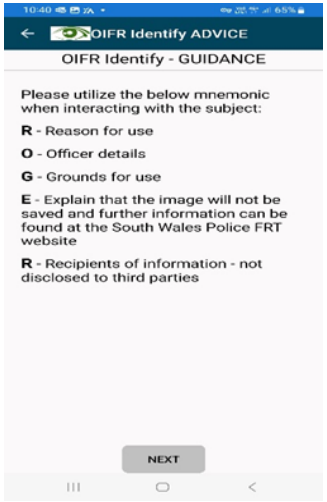
  Recipients of information – not disclosed to third parties

[16] https://www.college.police.uk/app/national-decision-model/national-decision-model
[17] Code of Ethics | College of Policing

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, will be supplied with an OIFR information leaflet or directed towards the SWP/GWP Facial Recognition website18 and privacy notice19 for further information.
Any person who requires additional information relating to OIFR will be provided with contact information for the SWP/GWP FRT team

(FRT@South-Wales.police.uk).

Figure 2. Initial guidance for officers on opening the API on force issued devices



[18] https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/ - to be updated
[19] https://www.south-wales.police.uk/hyg/southwales/privacy-notice/ - to be updated

Purpose Limitation

Body worn video (BWV) will be used to record the use of OIFR for audit purposes. No facial recognition technology will be used on the BWV and it will be utilised in accordance with current practices. BWV will be categorised on the appropriate evidence management system[20] in line with 'stop search' and 'use of force' policies[21]. Where BWV is not used the Operator must record on their electronic entry for use of OIFR why this is the case e.g. the equipment is broken.

This is in addition to the entries made on the app which require the Operator to record the reason and the grounds for use.

Retention

The OIFR app does not permit the Operator to retain the Probe Image or biometric template in the OIFR app or in any other storage format. The Probe Image is automatically deleted at the conclusion of the OIFR comparison and cannot be recovered.
Where a match occurs, the OIFR app will record the unique niche identification number for any possible matches returned but neither the Probe Image or Candidate Images returned are not recorded in the OIFR app or any other system.

Security

Accountability

Governance and oversight of the use of the technology is approached in three stages, as follows:
a) Pre-Operational use;
b) Operational Use
c) Post-use.

[20] NICE Investigate
[21] Internal policies can be provided on request

a). Pre – Operational Use

Prior to any use of OIFR, the Operator must have undertaken the relevant OIFR training provided by the force Digital Services Division. Access to the OIFR system will not be provided to Operators until this training has been completed to a satisfactory level. A record of training will be retained and if the pilot is successful, refresher training will be delivered at appropriate intervals.

Any decision to utilise OIFR will be the responsibility of the Operator to ensure the proportionality and justification of its use.

The outcomes of any OIFR searches, even those discarded before completion, will be automatically recorded in the e-pocket notebook (ePNB) of the Operator and will be available for review by the Operator, Supervisors and individuals authorised to review ePNB's for the purposes of oversight, governance and conduct matters. The entries in the ePNB of Operators are not amendable in order to ensure transparency and accountability of Operator use.

A number of other specific SWP/GWP documents pertaining to use of OIFR have been completed centrally. These are set out below:

Key Documents Available to the public	Information provided
SWP/GWP OIFR Legal Mandate	The lawful basis for processing data in relation to OIFR. Including in relation to: • Common law policing powers • Human Rights Act 1998 • Equality Act 2010 • Protection of Freedoms Act 2012 • Data Protection Act 2018 & UK GDPR • Freedom of Information Act 2000
SWP/GWP OIFR Policy Document	A statement of intent setting out principles for the use of OIFR and how personal data will be processed. Data retention periods applicable to OIFR
SWP/GWP OIFR Data Protection Impact Assessment (DPIA)	Assessment for the identification and mitigation of privacy and information security risks of OIFR
SWP/GWP OIFR Appropriate Policy Documents- Part 2 and Part 3 processing	Explanation of the procedures for securing compliance with the principles in Article 5 UKGDR and s.42 Data Protection Act 2018 and satisfies Schedule 1 Part 4 of the Data Protection Act 2018
SWP/GWP FRT Equality Impact Assessment	Assessment to ensure compliance with the Equality Act 2010 and the Public Sector Equality Duty

b) Operational Use

The Operator will have an interaction with the Subject, unless is not possible for this to occur (for example the Subject is deceased), for a lawful policing purpose. During the course of this interaction, the Operator may form the belief that it is necessary for the Subject to be identified in order that relevant checks can be undertaken or appropriate actions be address. The Operator should make all reasonable efforts to identify the Subject via traditional, less intrusive means. It will also be the responsibility of the Operator to ensure prior to any use that they are lawfully on premises for the lawful policing purposes.

At the outset of an OIFR search (*see Figure 1 above*), the OIFR app will automatically create an entry in the ePNB of the Operator. This entry will record:

- the date of the search;
- the time;
- whether the search was conducted in a public or a private place (see *figure 3*);
- the demographics of the subject (including Officer defined Gender, Age and Ethnicity);
- the circumstances justifying the search, the reason and grounds for the search;
- the Image Reference Database(s) the search was conducted against; and
- the location of the search

Figure 3

As referred to above there must be both a reason and grounds for use which must be recorded – see figures 4 and 5.

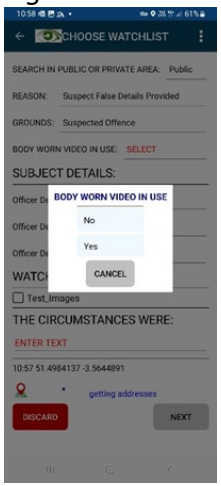
Figure 4

Figure 5

The Operator will capture a suitable Probe Image using the camera on their force issued mobile device for an OIFR search to be undertaken and will use the cropping tool included in the OIFR app to ensure collateral inclusion is minimised or eliminated where possible.

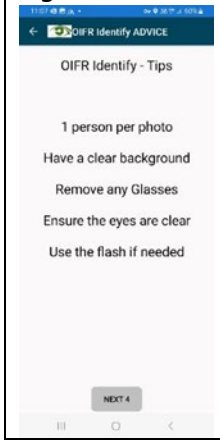
The OIFR search will be undertaken with body worn video being utilised to record the interaction. Where body worn video is not used the Operator must make a note in the ePNB why this was the case (*figure 6*.). Reasons for non-use of body worn video will be addressed under operational business as usual procedures.

Figure 6



After selecting the Grounds, Reason, Image Reference Database(s) and Location of the search completing the mandatory fields as above, the Operator will be shown the below 'Top Tips' page (*figure 7*), offering guidance on obtaining the best image possible and minimising the impact of environmental, subject and system factors that may impact the OIFR app's ability to recognise the Subject's face.

Figure 7.



The OIFR app has been configured to ensure any Probe Image captured via the mobile phone camera through the OIFR app remains within OIFR and cannot be saved to any other location. Once the search is completed, that image is not stored on the device in any way and is not retrievable. Other basic functionality of the standard mobile phone camera (flash, zoom etc) is available to the Operator.

Once a Probe Image has been captured, it will be presented to the Operator to ensure it is sufficient quality for comparison (no blurriness, glare or poor lighting). A 'retry' option is provided, for use if the Probe Image obtained is unsuitable, for example blurred or obscured. On selection of 'retry', the previous image is deleted. The Operator is then offered the opportunity to 'crop' the image as necessary to ensure only the Subject's face is included in the Probe Image and collateral intrusion is eliminated.

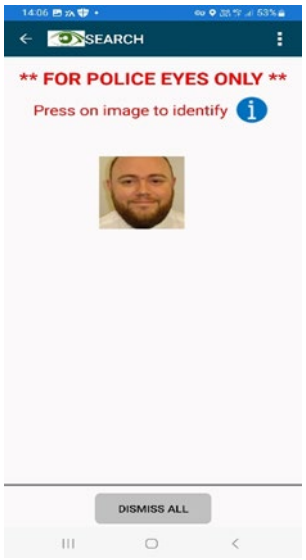
When the Operator has obtained a suitable image, selecting the 'SEARCH' option will initiate the search comparison process, searching against the selected Image Reference Database(s) selected on the previous page.

The OIFR Probe Image which has been taken is not stored within the device or retained within the OIFR app, the SWP/GWP mobile phone, or in the iPatrol application.

The OIFR app will return maximum of up to 6 Candidate Images that exceed the OIFR Threshold Setting for the Operator to consider. At this stage no other details accompany the Candidate Image. The Operator must select an image for any other details to be presented (*figure 8*).

To note - **If searching against the custody Image Reference Database, there may be multiple Candidate Images of the same person returned to the Operator as the custody Image Reference Database contains separate images from each previous detention for any person included.**

Figure 8



If there are no images that return a Similarity Score above the Threshold Setting, then the results will automatically be dismissed and the Operator will receive an on screen message stating 'No Results Returned'.

The Operator will review the Candidate images returned and make a determination if a match has been made, ensuring that there is a 'human in the loop' decision.

Upon selecting a Candidate Image that the Operator considers is a possible match, the Operator will be able to view the Probe Image and Candidate Image side by side on their device for comparison. With identification details available only at the point of selection, the Operator can then access additional information on the relevant police systems (niche, warrant management system or PNC) dependant on the grounds for use, as per existing operational procedures

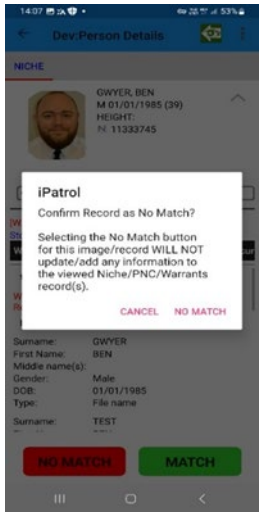
To ensure that use of OIFR can be properly audited and provide appropriate transparency and oversight, a mandatory audit requirement is included.

This takes the form of two buttons 'NO MATCH' and 'MATCH' which feature at the bottom of the Person Details screen. Selection of one of these buttons is mandatory to record the outcome of any search performed as a result of OIFR.

No Match

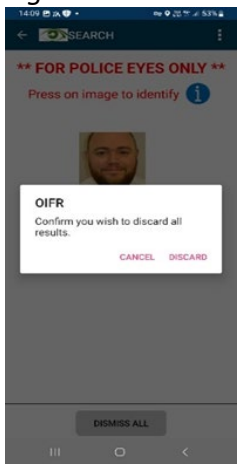
If the Operator decides as a result of searching the details of a Candidate Image that the Subject has not been successfully identified, 'NO MATCH' must be selected. This will prompt the Operator to confirm that this Candidate image is not a match to the Subject (*Figure 9*). This will return the Operator to the original Candidate Images however with the previously chosen Candidate Image now greyed out.

Figure 9



If the Operator determines that none of the Candidate Images returned matches the Subject, the Operator should select 'DISMISS ALL'. (Figure 10). The user is then asked to confirm that they wish to discard all results. At this point, the Probe Image will no longer be accessible for further searches or 'side-by-side' comparison of the Probe Image against any Candidate Image. The Probe Image and associated Biometric Template will be automatically deleted by the OIFR App.

Figure 10



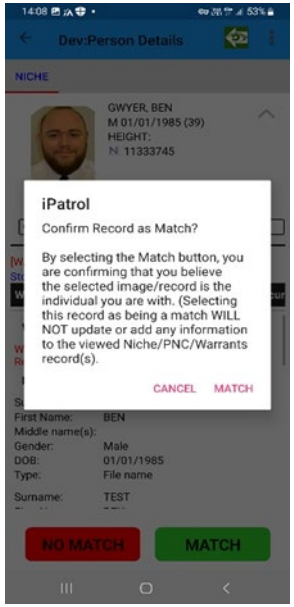
An ‘additional information’ free text box is presented for Operators to capture any other information relevant to the OIFR search. The Operator presses ‘COMPLETE’ at the bottom on the screen, the use of the OIFR app is now concluded. (*Figure 11*)

Figure 11

Match

If the Operator selects the 'MATCH' option, the Operator is presented with a confirmation selection to confirm that the Operator believes a match has been made (*figure 12*). If this has been selected in error, the Operator has the opportunity to 'cancel' the 'match'.

Figure 12



Where the Operator confirms that they believe a match has been made the OIFR app will present a returns form to capture the outcome of the match. The 'Outcome of positive match' field is mandatory for completion by the Operator.

Upon selecting 'Match', the Probe Image will no longer be accessible for further searches or 'side-by-side' comparison of the Probe Image against any Candidate Image. The Probe Image and associated Biometric Template will be automatically deleted by the OIFR App. An additional 'Outcome of Positive Match' picklist is included. (*figure 13*) This presents a drop-down list with possible outcomes for the Operator to select and document. (*figure 14*).

Figure 13

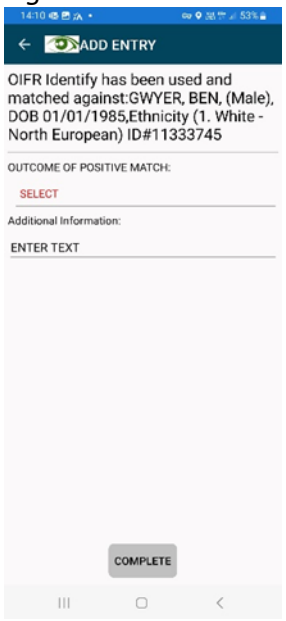
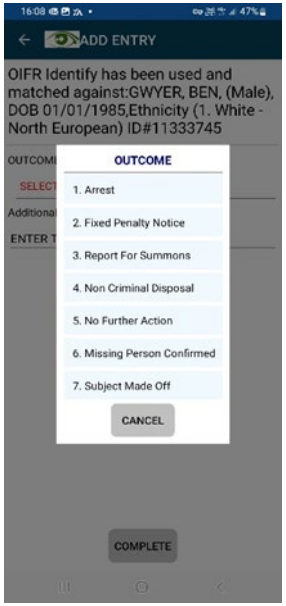


Figure 14



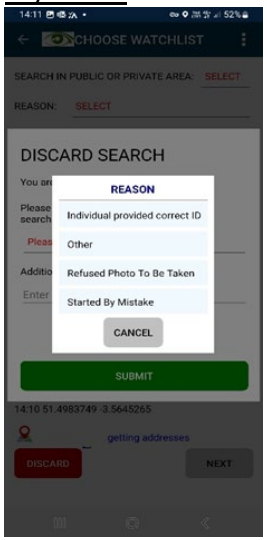
Upon selecting an outcome, the Operator selects 'Complete' and the use of the OIFR app is concluded.

For both matched and non-matched images the officer will detail in the freetext field any concerns raised by the Subject, if appropriate further relevant details pertaining to the disposal and any other information that might be relevant to OIFR use.

If the Operator exits from the OIFR app before the search is completed, the Operator will be presented with a mandatory screen to record the reason for abandoning the search (*figure 15*). The reasons for the search being discarded will be:

- started by mistake,
- individual provided correct identification,
- subject refused to have image taken, and
- other (selecting this option presents a mandatory free text box for the Operator to record the reason).

Figure 15



Post use

Effective auditing and accountability with regard to use of OIFR is of paramount importance, to ensuring transparency and maintaining public confidence.

Any use of the OIFR app automatically generates an audit log which is recorded in the Operator's ePNB (*figure 16*). The Operator has no means to edit, or modify or delete the automated entries generated in their ePNB by the OIFR app however if required for the purposes of clarity, the Operator could supplement the entries with a further ePNB entry if information was required or pertinent.

Figure 16. Search initiated time and date stamp

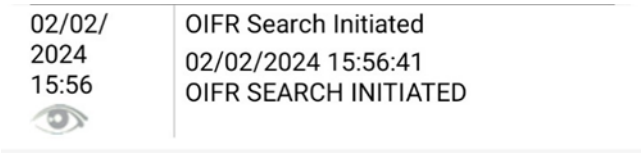


Figure 17. Operator inputted details log

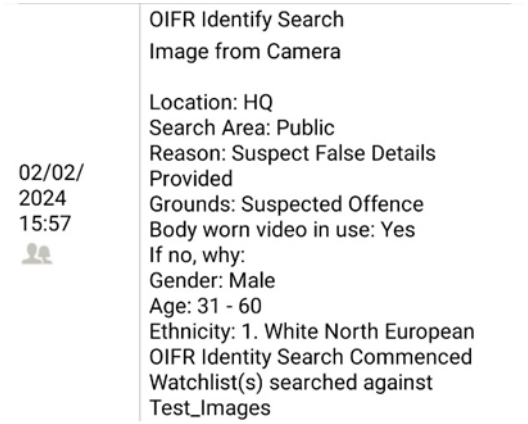


Figure 18. Search results log

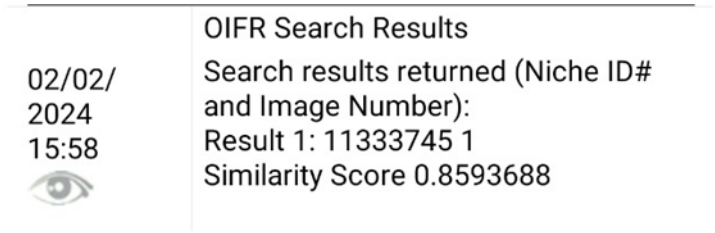


Figure 19. Viewed candidate records log

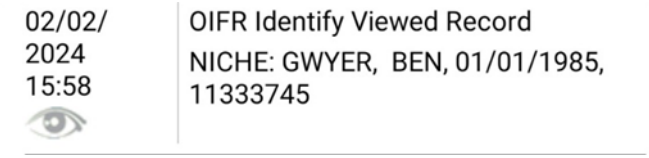


Figure 20. Identify Match log (free text)

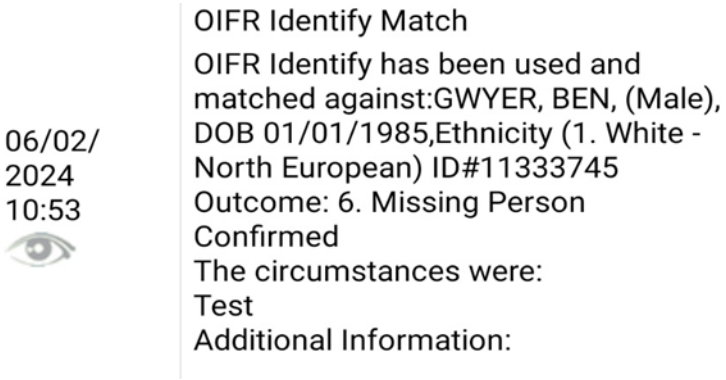


Figure 21. No Match log (free text)

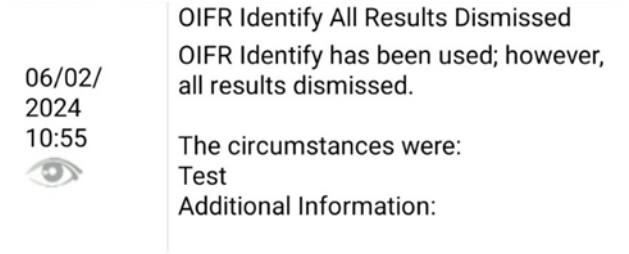
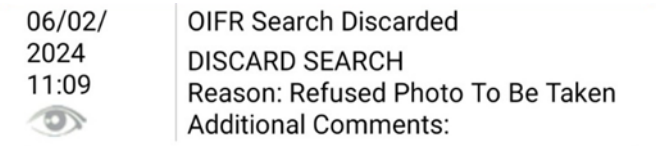


Figure 22. Search Discarded log



The automated completion of ePNB entries provides an audit function that allows use of OIFR to be monitored and evaluated.
The Operator will be responsible for ensuring that BWV recordings of their interaction with the subject are properly categorised and retained as per existing operational procedures.

SWP/GWP will ensure that the processing of any personal data associated with OIFR is conducted in a lawful way in compliance with SWP/GWP OIFR Documents. This includes that:
a) Probe image as captured by OIFR is immediately deleted in the OIFR Device and FRT System; and
b) Biometric Template of Probe Image is immediately deleted in the FRT System.

The Supervisor of the Operator will undertake periodic reviews of the searches conducted by the Operators on their team to ensure compliance with policy and to ensure searches are ethical, justified and proportionate.
The outcome of OIFR uses must be subject of ongoing evaluation, which in turn should feed into oversight and scrutiny processes

Part 2 – Image Reference Database

Insights indicate that significant criminal offending in South Wales is local and repeat and so comparing potential Probe Images of Subjects against SWP/GWP custody database is considered a relevant tactic when trying to identify a Subject. The custody database contains images of individuals who have been arrested. No victim or witness images are available.

Officers will not be in a position to anticipate individuals that they may encounter nor locations that they will attend during their shift (whereas a deployment of facial recognition would be targeted and intelligence-based determining the make-up of a watch list). In addition, currently it is not possible to generate lists based on separate categories of subject (e.g. on bail, prison recall etc) due to the fast-paced nature of change in the status of subjects but also due to current technological capability. If it were possible, an officer would be required to have an indication of information which can only be accessible when the subject has been identified.

Under the Police and Criminal Evidence Act 1984 Code D[22], section 64A of PACE provides the police with powers to take photographs of suspects to be used in the prevention or detections of crime, the investigation of offences or the conduct of prosecutions. Section 5 of the Code refers to detainees at a police station and provides the power to search and examine them for the purpose of establishing their identity. They may be searched and

[22] HYPERLINK "https://assets.publishing.service.gov.uk/media/65816ec7fc07f300128d4433/PACE+Code+D+2023.pdf"Police and Criminal Evidence Act 1984 (PACE) – Code D Revised Code of Practice for the identification of persons by Police Officers

examined to establish whether they have any identifying marks, features or injuries that would identify them. By identifying a Subject in real time using OIFR this intrusive and time-consuming process may be avoided.

Section 5.12 allows for photographs to be taken of detainees without their consent. The notes for guidance under section 5B(c) states:

"when the real identity of the person is not known and cannot be readily ascertained or there are reasonable grounds for doubting a name and other personal details given by the person, are their real name and personal details. In these circumstances, using or disclosing the photograph to help to establish or verify their real identity or determine whether they are liable to arrest for some other offence, e.g. by checking it against other photographs held in records or in connection with, or as a result of, an investigation of an offence".

Points to note:

- In order to avoid being arrested individuals may claim a different identity;
- The above scenarios require a subject to be arrested, which is intrusive, is likely to be in public and is time/resource intensive therefore interfering with the Subject's privacy, which, whilst reasonable at the time, may turn out to be unnecessary on identification;
- All crime records will be available to officers for further investigation into the individual's identity resulting in the viewing and accessing of multiple records to achieve this aim.

By enabling OIFR to match biometric templates held on the image database in real time these points can be avoided:

- Where there is no match, a subject may not be detained or arrested in public;
- Where there is no match less time and resource will be required to confirm this, enabling better provision of officers on the frontline;
- The amount of personal data and special category data accessed and viewed in order to identify an individual will be reduced. This information is available to officers in any event, as part of their role-based access to crime records for which they are vetted and trained.

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*
Subject – image, location, officer identified gender, age group – where there is a match this will provide access to specific details such as, but not limited to full name, aliases, date of birth, address, previous addresses, criminal convictions (if held).
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 ☒ Criminal Convictions or offending data ☐ None Comments:

Data Subjects: What categories of data subject are involved?
☒ Persons suspected of having committed or being about to commit a criminal offence ☒ Persons convicted of a criminal offence ☒ Persons who are or may be victims of a criminal offence ☐ Witnesses or other persons with information about offences ☒ Children or vulnerable individuals ☐ Police officers or staff (current and former) ☐ Other If other, then please provide further details below:

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?

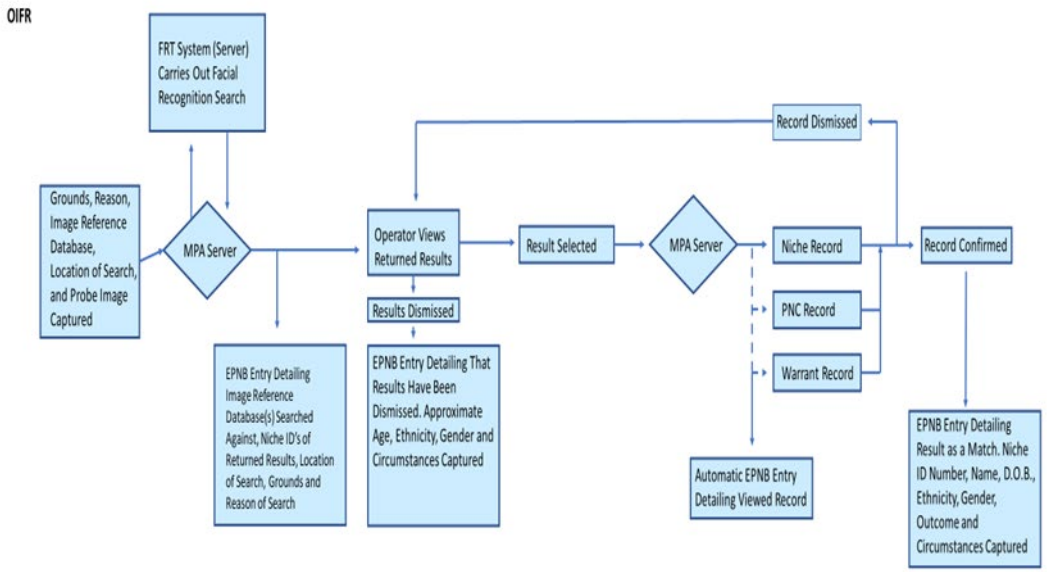
Will you be collecting new information about individuals?

Collection	**SUBJECT:**	**IMAGE REFERENCE DATABASE:**
Method – manually input.	An image will be captured by an officer manually taking a photograph of a Subject who has refused or is unable to identify themselves where specific grounds are met, using the OIFR app on a secure force issued smart phone.	Where an individual is taken into custody a photograph is taken of them and placed on police systems. Photographs of missing persons will be provided by friends/family or associates and also placed on Police systems. In some
Source – by super users		

Privacy Info Other Info	The source of the image will be the subject themselves. The subject will be informed that their image will be taken so that a biometric template will be compared to those on the Image Reference Database(s) as a result of their refusal or inability to identify themselves. The individual will also be informed of the reason and grounds for use of OIFR. They will be directed to the force privacy notice, the SWP/ GWP Facial Recognition website and provided with a leaflet containing information if requested. Where the subject asks for a contact to enquire about OIFR they will be provided with the Facial Recognition Team email address. The supplier of the biometric algorithm and the public sector equality duty in relation to the algorithm has been discussed in the Live Facial Recognition DPIA (256) therefore this will not be covered in this DPIA. The Live Facial Recognition DPIA can be provided on request or is accessible via the SWP Facial Recognition website. The security of police systems and devices is not within the scope of this DPIA.	cases, images will be provided by other police forces and organisations due to the transient nature of crime and individuals at risk. The images are duplicated to create the Image Reference Database for OIFR. Where an individual has their photograph taken in custody the image will be 'seen' by the FRT system and ingested into the Image Reference Database. The images are captured for policing purposes and the further processing for the purpose of identifying specific cohorts also for policing purposes is considered to be not to be incompatible with the original purpose**.** Due to the changing status of individuals as they move through the justice system it is not currently possible to categorise the images within the database in order to compare the Probe Image of a Subject against a specific cohort, reducing the number of images used in the processing. SWP/GWP acknowledge that some images may be unlawfully held. This is a national issue which is currently being addressed by Programme Tabula.

Information flow	Description *(provide details where applicable)*
Method of transfer	The subject's biometric template will be transferred via a secure application programming interface which is a set of protocols that enable different software components to communicate and transfer data. The API is created and located within the force secure VPN and is accessed via secure force issued mobile devices which must be accredited to national security standards.
Where to	Secure Facial Recognition Servers within the SWP secure network (DPIA256)
Access/permissions	Operators: Operators will only receive access to the OIFR app on successful completion of the mandatory training and whilst remaining in compliance with any mandatory refresher training at appropriate intervals. Permission to use the OIFR app can be removed instantly and remotely should there be any concerns regarding the manner in which the technology is being used by the Operator. Operators do not have permission to add images to the Image Reference Database, amend records or delete any persons within the Image Reference databases. Facial Recognition Administrators: This is a role-based access provided to a limited number of specifically vetted Officers and staff. These persons will have authorities to make amendments to the Facial Recognition system where specific authority is given and any amendments will be logged and referred to the Facial Recognition Programme Board at the earliest opportunity for agreement or in the event of urgent action being required, escalated to the Senior Responsible Officer for ratification.
Aggregation	n/a
Sharing	No information processed as a result of the image capture or biometric matching is shared with third parties
Storage	The Image Reference Database resides within the SWP Facial Recognition Technology Servers. No images or biometric templates are retained on the mobile devices
Retention	On initiating a search, the OIFR Probe Image of the subject which has been taken is not stored within the device or retained within the OIFR app, the SWP/GWP mobile phone, or in the iPatrol application. Upon selecting 'Match', the Probe Image will no longer be accessible for further searches or 'side-by-side' comparison of the Probe Image against any Candidate Image. The Probe Image and associated Biometric Template will be automatically deleted by the OIFR App. If the Operator determines that none of the Candidate Images returned matches the Subject, the Operator should select 'DISMISS ALL'. (Figure 10). The user is then asked to confirm that they wish to discard all results. At this point, the Probe

	Image will no longer be accessible for further searches or 'side-by-side' comparison of the Probe Image against any Candidate Image. The Probe Image and associated Biometric Template will be automatically deleted by the OIFR App
Additional information	To ensure the integrity of the images in the custody and missing persons database and the duplicate Image Reference Database on the Facial recognition Servers each image is applied a hash value which is compared on a daily basis.
Recorded	See Figure 1-22 above
Additional integrated technologies	FRT Technology (DPIA256), OIFR API, Niche RMS, Image Reference Database, iPatrol app – Electronic Pocket Notebook
Auto delete/Manual deletion/overwrite	See retention above. The hash values on the image reference database will alert the FRT Project Team to any variances in the database e.g. an approved request for deletion of a custody image ensuring that image is removed.
Additional information about the process	Each step of the process is logged within the ePNB when the OIFR app is used. This documents all decisions, information and actions taken by the Operator. Where possible this is also documented via an officers' body worn video. All actions can be audited, and the information is monitored and evaluated to identify issues, measure success and ensure regulatory/legislative compliance of OIFR. Appropriate Police Documents will be available. Detailed Standard Operating Procedures and training will be provided to Operators. The pilot will be rolled out incrementally, increasing the number of Operators over the pilot period. The app has purposely been designed to account for privacy risks and data protection compliance and to enable Operators to navigate the National Decision-Making model which is in place across all police forces.

Diagram or process map	

How will the information be used?	
	Monitored in real time to detect and respond to unlawful activities
	Monitored in real time to track suspicious persons/activity
x	Compared to reference data of persons of interest through processing of biometric data such as facial recognition
	Compared to reference data of vehicles of interest through ANPR software
	Linked to sensor technology
	Used to search for vulnerable persons
	Used to search for wanted persons
	Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
	Recorded data disclosed to authorised agencies to provide intelligence
	Other: *(please specify below)*

Describe the context of the processing:
Who will be making decisions about the uses of the system and which other parties are likely to be involved?
Will you be sharing the information with other organisations or agencies? Records any other parties you would disclose the data to, for what purposes
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?

The use of the system has been determined by SWP/GWP to supplement existing police powers to identify individuals where certain circumstances exist. The decision to use OIFR on the frontline will be for the individual Operator who will be trained in the appropriate and proportionate use of OIFR, the Code of Ethics and the National Decision-Making Model. As set out above the decisions will be auditable and evaluated.

No information processed for the purpose of uniquely identifying an individual via OIFR will be shared with any third parties. This is a supplemental tool for existing policing purposes.

The police have common law powers which are deployed for policing purposes which are generally defined as:

- protecting life and property,
- preserving order,
- preventing the commission of offences,
- bringing offenders to justice, and
- any duty or responsibility of the police arising from common or statute law

The powers are carried out 'by consent' therefore the public expects the police to process information and personal data to this end whilst being accountable for doing so in a lawful, proportionate way. Where an officer considers the use of OIFR to be necessary where the reasons and grounds are present, the Operator will inform the subject of the intention to use it, why and what that entails. Further to the use of retrospective and live facial recognition this progression could be considered an expected step.

Initial use of OIFR will be supported by a communications strategy and privacy notices will be amended prior to use.

Children and Vulnerable People

In some cases, the processing may include children or vulnerable individuals however all information captured through deployment of OIFR is deleted.

The retention of images of children on the Image Reference Database are subject to shorter retention periods under the Management of Police Information (MoPI)

The Operator should take all reasonable steps to ensure the Subject of OIFR use understands what is being said to them. This is particularly pertinent to children under 18, persons who are vulnerable through diminished capacity or understanding or people who are unable to understand or communicate effectively in English. If there is any doubt that the Subject understands what is being explained to them, the Operator must take reasonable steps to ensure the understanding of the Subject and to bring relevant information pertaining to the use of OIFR to their attention. Reasonable adjustments the Operator should consider to support a Subject who is vulnerable could include:

- speaking slowly and clearly
- speaking in plain language or explaining things in different ways
- facing the Subject and allowing them to see the Operator's lips
- writing their question and allowing the Subject to write their response
- understanding the Subject not making eye contact
- allowing the Subject time to think about the question
- being patient to allow the Subject to articulate an answer
- using language line or other approved translation services to allow communication with Subjects whose first language is not English
- If the Subject is accompanied by a carer or other person who can support them, the Operator must try to establish whether that person can interpret or otherwise help the Operator to give the required information and also support the Subject in communicating any pertinent information or concerns

Welfare and Safeguarding of Children and Vulnerable People

If the Subject of OIFR use is found in circumstances that suggest their welfare and safety may be at risk, force safeguarding procedures should be initiated. This is especially pertinent for Children and vulnerable persons (as defined by College of Policing).
It is recognised that children under the age of criminal responsibility may be used by older children and adults to hold illegal items such as drugs and weapons and, in some cases, firearms or to undertake criminal activity for the criminal benefit of others. This criminal exploitation is often:
• in the hope that police may not suspect they are in possession of illegal items (knowingly or otherwise);

• knowing that if criminal offences are identified involving children or vulnerable people, they cannot be prosecuted for criminal offences.

Children under 10 should only be subject of OIFR use in exceptional circumstances and their safeguarding and welfare should be the immediate priority of the Operator.
Where it is necessary to do so, every effort should be made for the search to be conducted in a child-friendly location. The search should as a minimum take place in a safe and controlled area, a police station being preferable to the street or in a police vehicle. All OIFR use relating to children under 10 should be referred to the safeguarding team as a priority.

Lawfulness - This processing will be considered to be new and there are likely to be challenges and concern about its use. Civil Liberties groups have previously raised concerns about the use of biometric facial matching in law enforcement. These concerns have been addressed in part following the *Bridges* cases however OIFR will be at the discretion of individual officers and not subject to the oversight and approvals that precede deployments of Live Facial Recognition.

As demonstrated above, Operators will have all decisions and actions recorded in an auditable trail without any of the data being retained. There are clear reasons and grounds for use which must be present and documented before the next steps can be taken.

Interference with Human Rights - It is acknowledged that it is likely that use of OIFR will interfere with the fundamental right to privacy. The application of the Bank-Mellat 4-part test (above) supports the findings of the court in *Bridges* that use of facial recognition can be deployed for policing purposes in accordance with the law and therefore such interference can be justified. The purposes for which OIFR can be deployed are clear and specific and as mentioned, generates an audit trail. Where a subject complies with a lawful request to identify themselves to a police officer there will be no justification for OIFR. Where there is a refusal and there are both reason and grounds interference with Article 8 is proportionate. The subject will have been provided with the opportunity to comply with a legitimate exercise of police powers and will be fully informed of the processing which will follow and why. Reference to Article 11 is included in the sections above however for ease of reference OIFR is not designed to be used in densely populated locations and is intended to capture one image. Where collateral images are captured in the background the officer will crop the image to remove any others.

Function Creep – there are concerns OIFR will be used to monitor movements and actions of the public with no justification or may be used covertly. There are also concerns that the Police will retain all images taken to compile a database of all members of the public. As explained above no subject images or biometric templates are retained irrespective of whether there is a match with an image held in the Image Reference Database or not. The utilisation of the OIFR app requires full explanation of why it is has been used on every occasion.

Disproportionality regarding the Image Reference Database – there are concerns that comparing a Subject's biometric template against the entire custody database is disproportionate. This is explained above. Due to the transient nature of criminals and the fast changing status of those within the Justice system it is not currently possible to categorise the images according to the grounds set out for use of OIFR. In addition, where a subject either refuses or is incapable of identifying themselves it would not be reasonable for an Operator to guess which category the subject may fall under. This may also negate the benefits of effective policing in a more timely manner benefitting the wider public and those at risk.

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 unknown individual from potentially thousands of individuals from their face alone; use of OIFR assists the front-line officer identify, help or dismiss a Subject from their enquiries. This also removes the potential for disproportionate processing of information relating to persons who are not related to the Subject for the purposes of ascertaining the identification of the Subject for a policing purpose. To undertake this manually would be both disproportionate in terms of the amount of data an Operator would need to review and also the amount of time a Subject would potentially be detained for the purposes of discovering their identification.

Benefits and Impacts:
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? Are there any adverse effects from the processing?

The effectiveness of frontline police officers to identify a subject quickly and without needing to detain them unnecessarily or to apprehend others swiftly will benefit the police, other public services, the wider public, victims of crime and those in need of urgent help. OIFR would enable one officer to identify one unknown individual from potentially thousands by their face alone. The impact this would have on resourcing and demand by enabling more time to be spent in critical areas rather than administrative efforts to consult numerous records and personally identifiable data would be beneficial to all.

Due to the design of the OIFR app, there is minimal impact on the Subjects whose data is being processed. There will be more tangible impact on the individual if OIFR is not used, in terms of privacy, time, safety, justice or retention and accessing/viewing of personal data in available records whilst trying to identify a Subject.

OIFR will assist in reducing the number of persons 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 the Subject to allow for the expeditious notification of a next of kin and formal identification for Coroner's investigations. This will also reduce the number of occasions on which a potential next of kin is incorrectly sought to identify a Subject.

Step 3: Consultation

List the relevant stakeholders who have been consulted *(please indicate whether stakeholder is internal or external and their role/interest)*

Stakeholder consulted	Consultation method	Views raised	Measures taken
Information Commissioner's Office	E-mail; informal consultation; meetings	Concerns raised about OIFR in particular the strict necessity threshold, what problem OIFR is trying to solve, the lawful basis and the context in which it will be used. Also, the risk of false negatives should be considered and what threshold will be used for the algorithm	DPIA revised to cover all points raised. frt-equitability-study_mar2023.pdf
Surveillance Camera Commissioner's Office	Meeting	An overview of OIFR and how it will be used was presented to representatives.	No measures required
Gwent Police Independent Advisory Group		OIFR was presented to Gwent IAG for consideration of use cases, governance and oversight upon live deployment of OIFR. The panel were supportive of the launch of OIFR if a consistent approach could be established across SWP and GWP, and later any other Forces adopting the technology to ensure transparency and consistency of use.	
NIST/NPCC/NPL/HO	Equitability study		frt-equitability-study_mar2023.pdf
Public Perception Survey OIFR 2023	Public engagement and perception survey	52 Surveys were completed at Wales Airshow 2023 over the course of 2 days. • 96% of participants felt that the SWP's prospective use of OIFR was positive.	

		• 94% of participants had no concerns about SWP use of OIFR. • 98% of participants believe officers should be able to carry out an OIFR search. • 58% of participants believe PCSO's should be able to carry out an OIFR search. • 96% of participants believe OIFR should be used in public places. • 67% of participants believe OIFR should be used in residential premises. • 94% of participants felt that the use of FRT improves confidence in SWP. • Participants felt that improved communication, through face-to-face engagement and improved use of social media, SWP could improve confidence in LFR. • Participants felt that SWP effectively communicated their intention to use LFR appropriately through a combination of social media prior to the event and signage at an event. • Participants were generally supportive of Live Facial Recognition and supported its use in tackling criminality and protecting those vulnerable in our communities.	

		The participants in this survey were broadly supportive of the use of Facial Recognition Technology, including Live Facial Recognition, and believe it improves confidence in local policing. Participants were also supportive of the prospective use of Operator Initiated Facial Recognition, particularly by police officers, and are generally supportive of its use in public areas and private premises.	
South Wales Police Independent Ethics Group 14/12/2023	Briefing	Matter was discussed at Joint Ethics Committee in South Wales and the minutes of the meeting are available at: SOUTH WALES POLICE ROLE PROFILE The Committee supported the use of OIFR by South Wales Police. Their recommendations were that a College of Policing APP should be sought for the use of OIFR however understood that this was unlikely to be in place at the point of OIFR being launched. The Committee offered recommendations on the use of OIFR in public and private places, recommending that '*OIFR did not seem to present a disproportionate infringement of the right to privacy*' . The Committee did not consider it necessary to provide a more limited use case for OIFR in private spaces. The Committee stated:	

		'Given that the photograph taken in an OIFR is a headshot which occupies most of the photographic frame, the collateral intrusion seemed to be relatively minor compared to that which would follow the use of body worn camera in a private space. The Committee recommended that steps should be taken, where possible, to minimise collateral intrusion. For example, the photograph should be taken with the subject standing in front of a blank well or in other ways that do not capture the details of the private space. It was also noted that, if no match is found between the image and the database on the device, the image is automatically deleted immediately'. The Committee was asked to consider the data capture created automatically by the OIFR app that would be used to monitor compliance and scrutiny of use of OIFR by Operators. The summary of this oversight was that they could not identify any additional data that should be recorded in order to allow effective scrutiny of OIFR.	
Gwent Police Independent Ethics Committee 30/04/2024	Meeting	OIFR was presented to the Gwent Independent Ethics Committee who were supportive of the use of OIFR. The Committee asked to be updated periodically with progress of the pilot in	

		order to offer recommendations going forward.	

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 Part 2 will be applied to general processing i.e. missing persons where no criminal investigation is being undertaken Part 3 will be applied to Law Enforcement Processing To note policing purposes are covered by both Part 2 and Part 3	
Legal power to carry out processing e.g. statute, common law, court order etc. *(please provide details)*	Common law powers Police and Criminal Evidence Act 1984 Interference with Article 8 is addressed above.	
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*	**General: Personal data** ☐ Consent ☐ Contract ☐ Vital Interests ☐ Legal Obligation ☒ Public Task ☐ Legitimate Interests	**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

special category data please select a further condition. *ICO Guide to GDPR - Lawful Conditions for processing*		☐ Data has been made manifestly public by the data subject ☐ Legal claims ☒ Substantial public interest ☐ Health ☐ Public interest in Public Health ☐ Archiving
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*	**Law Enforcement: Personal data** ☐ Consent ☒ Processing is necessary for the performance of a task carried out for that purpose by a competent authority.	**Law Enforcement: Sensitive processing** ☐ Consent ☒ Processing is strictly necessary for the law enforcement purpose; **and** ☒ Statutory etc purposes ☒ Administration of justice ☒ Protecting vital interests ☒ Safeguarding of children and individuals at risk ☐ Personal data already in the public domain ☐ Legal claims ☐ Judicial Acts ☐ Archiving

Data Protection Act 2018 Schedule conditions for processing special processing or in the substantial public interest	Schedule 1 Special Categories of Personal Data and Criminal Convictions Part 2 Substantial Public Interest Conditions Para 5 Requirement for an appropriate Policy Document Para 6 Statutory etc, and government purposes Para 7 Administration of Justice Para 10 Preventing or detecting unlawful acts Para 18 Safeguarding of children and of individuals at risk Part 3 Additional Conditions Relating to Criminal Convictions Para 30 Protecting individual's vital interests Para 36 Extension of conditions in Part 2 of this Schedule referring to substantial interest Part 4 Appropriate Policy Documents and additional safeguards Schedule 8 (1) Statutory etc purposes Schedule 8 (3) Protecting individuals' vital interests Schedule 8 (4) Safeguarding of children and 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.	This DPIA considers the utilisation of OIFR as an overt tactic and will be supported by a Communications Strategy to provide information to the Public. 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. (See figures 1-22 above)

<table>
<tr><td></td><td colspan="4">The Operator will explain that the Subject's Probe Image will be immediately and automatically deleted at the conclusion of the OIFR comparison and not shared with any third party.

Information regarding officer identified age, ethnicity and gender will be recorded by the Operator for the purposes of auditing the use of OIFR to ensure use is ethical and proportionate. Information added to the ePNB automatically as a result of OIFR will be 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</td></tr>
<tr><td>Will the personal data collected be used for any other purposes? (Please provide details)</td><td colspan="4">No. The image and biometric template is deleted.</td></tr>
<tr><td rowspan="5">Will the processing include mechanism to facilitate the exercise of individual rights (please select which rights can be exercised)</td><td>Right to be informed</td><td>x</td><td>Right to restriction of processing</td><td>x</td></tr>
<tr><td>Right of access by data subject</td><td>x</td><td>Notification of erasure, restriction or rectification</td><td>x</td></tr>
<tr><td>Right to rectification</td><td>x</td><td>Right to data portability</td><td></td></tr>
<tr><td rowspan="2">Right to erasure (right to be forgotten)</td><td rowspan="2">x</td><td>Right to object</td><td>x</td></tr>
<tr><td>Automated decision making, including profiling</td><td></td></tr>
<tr><td>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?</td><td colspan="4">Subjects – 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 and independent academic equitability testing undertaken by the National Physical Laboratory (NPL) has shown that there is no identifiable bias across any of the demographics tested, with equitability being seen across all groups tested.
A link to the findings of the NPL study can be accessed via:</td></tr>
</table>

	frt-equitability-study_mar2023.pdf (science.police.uk) 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 an 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. The software company is only involved in the development of the Ipatrol and the OIFR app. The software company does not have access to data held in the record management system or the ability to alter, amend or delete data held. iPatrol is accessible to SWP/GWP officers since 2015 via their Police issued 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's ePNB cannot be amended or deleted by the Operator however the Operator can supplement the search with further free text if there is further information pertaining to the search. The Image Reference Database has an applied hash value to maintain the integrity of the database from the custody database. Any variations in the hash value is notified to the Project team for rectification. Custody Images are subject to a national review – Programme Tabula Individuals whose data is held on police systems can make a request for deletion which is under the discretion of Chief Constables.
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 initial image and biometric template of the subject is not identifiable. The processing of the biometric template is for the purpose of uniquely identifying a living individual and is therefore considered to be special category data. The result of a positive and confirmed match will be 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 group, perceived gender and perceived 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 and reporting under the Equality Act 2010. There is likely to be significant public interest in use of OIFR. 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 OIFR use.	
Retention	How long will the data be retained in an identifiable form?	The Subject Image and biometric templates will not be retained. The Candidate Images on the image reference database are retained in accordance with Management of Police Information (MoPI) retention periods.
	Why is the data retained for this period?	Custody Images are retained in accordance with Management of Police Information retention periods.
	What reviews of the data will take place?	Reviews of custody images are undertaken in accordance with Management of Police Information retention periods.
	How will the data be disposed of?	Subject Probe Image and biometric templates are disposed of automatically and immediately on conclusion of OIFR use. Custody images are removed from police systems. The Image Reference Database is a replica of the images on police systems with an applied hash value to enable to the Facial Recognition team to identify images for removal

	Are backups subject to the same process as above?	Yes
	If not, please provide details	
How will you ensure that the processing is limited to its lawful purpose and that only the minimum data that is necessary for that purpose is captured?	Figures 1-22 above demonstrate how processing is limited for the specific reasons and grounds with only the minimum data captured by design.	
Transfers outside the UK	Location and recipient details	n/a
	Environment (e.g. on premise, cloud)	[redacted]
	Reason for transfer	
	Safeguards	
	Does the above also apply to any backups?	
	If not, please provide details	
Information Sharing	No personal information will be shared with third parties. Information regarding the monitoring and evaluation of OIFR use will be shared with academic partners and evaluators and 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. A contract is in place with the algorithm supplier.	
Information Security		
What police system(s) is involved in this processing?	Niche RMS, iPatrol (ePNB), Facial Recognition Technology Servers (SWP on premise)	
Is data encrypted in transit? If yes provide details	Yes, the information is transferred between systems on an accredited secure closed VPN. Delivery of OIFR is via a secure application used to manage SWP/GWP mobile phone assets	
Is data encrypted at rest? If yes provide details	Yes, any information is stored on systems an accredited secure closed VPN.	
What access controls are in place? If yes, please provide details of who will have	Access to the OIFR app will only be made available to frontline officers who complete the OIFR training to a satisfactory standard. If there are any concerns raised regarding the manner and use of OIFR by	

access to data and what controls will be in place?	the Operator, permission to use the OIFR app can be removed with immediate effect and remotely until such a time as those concerns have been addressed. Access to NICHE RMS to obtain further information following a positive match is assigned to officers and staff dependant on their role, vetting and training. 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. 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).
Is the force data segregated? Provide details	n/a
What audit arrangements are in place for use of the system?	All use of OIFR will be recorded in the Operator's ePNB. See figures 1-22 above.
What training will be provided to users?	Bespoke training for officer will be rolled out prior to any enabling of the OIFR app on officers' force issued devices and delivered by the SWP/GWP Digital Services Division. 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 Annual Management of Police Information and Data Protection training is mandatory for all staff and officers	
Level of vetting for contractors (including support & maintenance)	n/a	
Details of security measures in place where data is held	Local arrangements for police systems are in place.	
How will the product connect to police systems?	Via Secure API within the SWP Secure network	
Data held on third party systems *(Redacted results of penetration testing will need to be provided)*	Penetration test conducted?	n/a
	Date of last penetration test?	[redacted]
	Has system been subject to a security breach?	
SOC *(Third party cloud based only)*	Does third party have SOC accreditation?	
Certifications *(e.g. ISO27001, provide details including scope – copies to be provided)*	[redacted]	
Has the Joint Supplier Questionnaire been completed?		

What other less intrusive options have been considered?	
Solution	**Reason why this is not suitable**
n/a	Traditional methods are resource intensive and not efficient

Policies -*are there written policies specifying the following*		
X	**Requirement**	**Details**

	Agencies/organisations that are granted access	
x	How information is disclosed	OIFR Policy, SOPS, Overarching Privacy Policy, Privacy Notices
x	How information is handled	OIFR Policy, SOPS, Overarching Privacy Policy, Privacy Notices
Y/N		
Y	Are these made public??	Privacy notices are public facing
Y	Are there auditing mechanisms?	All entries on the ePNB via the OIFR App are auditable
	If so, please specify what is audited and how often	Supervisors of Operators granted access to OIFR should be undertaking reviews into the use by their staff at least monthly if not more regularly to ensure that use is ethical and in line with policy. Divisional management oversight will fall in line with similar review periods to monitor compliance and outcomes. Force level scrutiny boards will review the data at least quarterly to ensure that scrutiny is sufficient and that sufficient oversight is in place to ensure effective management of the use of this technology. FRT Programme Board will assess the effectiveness of use of OIFR including any patterns of disproportionality, consideration of accuracy and bias in the deployment of OIFR in uncontrolled operational environments (varying lighting conditions, Operator competence and other factors that could affect the reliability of results returned), outcomes of the comparisons and reviews of perceived benefits of use.

Step 5: Identify and assess privacy & compliance risks *Please identify all risks for each section*							
No.	**Identify risk – Cause, event, effect**	**Likelihood (L, M, H)**	**Impact (L, M, H)**	**Risk (L, M, H)**	**Mitigating measure**	**Residual Risk (L, M, H)**	**Accepted/ Rejected**
R1 **Vulnerability when data in transit** (Consider risk from various threats from hackers such as Foreign Intelligence services, Serious and Organised Crime, and individual hackers for example, force data transiting networks should be adequately protected against tampering and eavesdropping)	As a result of the biometric template being transferred from the app to the SWP FRT servers there is a risk that it could be intercepted or interfered with by threat actors leading to a compromise of the data and/or threat to police systems which in turn could affect the confidentiality, availability and integrity of all police held information	L	H	M	The OIFR API and the on prem servers are all within the secure SWP VPN. No data is transferred outside of this network which is accredited to national security standards	L	
R2 **Vulnerability when data at rest** (Consider risk from various threats from hackers such as Foreign Intelligence services, Serious and Organised Crime, and individual hackers for example. A malicious or compromised user of the service should not be able to affect the service or data of another.	As a result of information being stored on mobile devices there is a risk that it could be accessed, there is a risk that it could be intercepted or interfered with by threat actors leading to a compromise of the data and/or threat to police systems which in turn could affect the confidentiality, availability and integrity of all police held information	L	H	M	The OIFR API and the on prem servers are all within the secure SWP VPN. No data is stored outside of this network which is accredited to national security standards. Force issued mobile devices are encrypted and have multiple password/PIN access requirements and timeout screen locks. Devices can be	L	

					deactivated and wiped remotely. No images or biometric data is stored on the device. All information is within the force secure network.		
R3 **Physical Security** (Force data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure by malicious or disaffected individuals who have indirect access to information; An individual who has no authorised access to police business information/ system, such as a cleaner, maintenance personal)	There is a risk that an individual may seize a force issued mobile device from an Operator leading to access to the device resulting in unauthorised access to information which may pose a risk to others.	M	M	M	Officers are trained to manage their own physical protection. In the event that this occurs when an Operator is utilising OIFR there are no personal details available even at the point of a positive match. The biometric data will not be available to the individual and access to further information requires additional authentication before the screen timeouts and locks rendering it inaccessible to unauthorised individuals.	L	

	There is a risk that the Operator, members of the public or the subject may suffer physical harm if OIFR is not used leading to a delay in critical information being accessed resulting in physical harm	H	H		The pilot will enable Operators to identify subjects who pose an immediate danger to others and themselves in a timely manner without unnecessary delay	L	
R4 **Personnel Security** (Malicious or Disaffected individuals who have direct access to information; An individual who has authorised access to police business information/system, such as approved user with limited privileges)	There is a risk that force officers or staff may use OIFR to identify individuals where it is not necessary for a policing purpose leading to unlawful processing of personal and special category data resulting in loss of confidentiality.	L	M	M	All use of OIFR is automatically documented and is auditable (see figures 1-22 above) therefore steps taken even where the app is used accidentally is recorded. In addition, wherever possible use of OIFR should be supported by body worn video with officers being held to account in any event. Officer and staff have access to police records under existing arrangements	L	
R5 **Malicious or Disaffected individuals who have privileged access to information;** (An individual who has privileged authorised access to police business information/system, such as IT administrator/system owner)	As R4						

R6 **Commercial Service Providers/ Suppliers** (Access to systems and information through an attack by the employees of the service provider either malicious or accidental. Consider how 3rd party accesses service for maintained for example.).	There is a risk that the supplier of the algorithm may fail to ensure that any bias or discrimination is eliminated as far as possible resulting in inaccurate identification of individuals leading to false arrests, unlawful interference with Article 8 rights, and targeting of minorities unfairly	L	H	M	The algorithm was tested by National Physical laboratory to determine the most appropriate settings to mitigate or eliminate bias towards any demographic. Whilst this testing attempted to replicate the realism of operational environments, it is recognised that there are variables such as lighting etc in the operational environment that cannot be controlled and could not be tested in a non-operational environment. SWP/ GWP have accepted the recommendation of the National Physical Laboratory to set the threshold at 0.66. During the pilot period, the Facial Recognition Project Team will intrusively monitor searches to determine the Threshold setting is appropriate. This will include a review of the number	L	

					of searches returning positive matches, those returning negative matches, the circumstances in which the searches have been conducted (conditions/ locations etc) and the Similarity Scores returned for any searches to the Operator (leading to both positive and no matches).		
	There is a risk that the supplier may gain access to the data used for OIFR resulting in compromise and loss of confidentiality leading to a loss of public confidence and trust	L	H	M	The supplier does not have access to any SWP/GWP information or any data captured or used as part of OIFR	L	
R7 **Accidental Disclosure** (The disclosure of information by staff either by careless talk or by allowing police business information to be viewed by unauthorised persons, through inadequately trained or inexperienced staff)	As a result of the Operator identifying an incorrect match there is a risk that third party data may be disclosed leading to a loss of confidentiality	L	M	M	The operator will not solely rely on the images presented to confirm any additional details. OIFR is an aid to identification however the officer will engage with the individual to establish whether a match has been made in the event that they are not sure that the subject is the correct individual. No action will be taken on the basis of an image.	L	

	As a result of an Operator not following the guidance and training there is a risk that the images identified as a possible match may be made visible to the subject resulting in unauthorised disclosure of candidate images	L	M	M	The OIFR provides prompts to the Operator. If a possible match is returned from the Candidate Image Reference Database the screen presented to the Operator is marked in red "For police eyes only" (see Figure 8). This will also be included in the SOPS and training	L	
R8 **Environmental threat** (Risk of fire, flood, explosion etc.)							
R9 **Other** (explain other threats that have been identified as part of the Risk Assessment process)	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	L	H	M	A communications strategy will be in place prior to OIFR launch to ensure that all available means of communicating that SWP/ GWP Operators will be using OIFR 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 utilise OIFR are based on firm evidence and transparent analysis.	L	

	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	H	M	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. The rationale documented by Operators will be subject of scrutiny at operational and force level to ensure compliance. In addition, the design and functionality of OIFR means that it is not suited to use in densely populated areas.	L	
	As a result of incorrect matching there is a risk that an individual may be incorrectly arrested leading to loss of liberty, complaints and enforcement action	L	H	M	A decision to arrest a subject is not solely based on a facial image match. Failure to allow an Operator to capture an image does not constitute a	L	

					criminal offence and an arrest may not be made based solely on the failure of a Subject to comply with the OIFR process, however this might support other aspects of the necessity to arrest. If the subject Image is incorrectly matched against image reference database this may result in an unlawful arrest. This risk is reduced by the Threshold Setting of 0.66 being implemented in line with guidance from the NPL Equitability Study. The risk here is no more prevalent than in current police practices when interrogating police indices and Operators should make all reasonable enquiries to corroborate any potential matches based on the information presented to them.		

					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.		
	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 leading to regulatory action.	M	H	H	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	L	
	As a result of the delay in updating the Image Reference Database there is a risk that some vulnerable individuals may not be identified leading to increased harm	L	H	M	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	L	
	As a result of potential incomplete deletion exercises there is a risk that Image Reference Databases	M	H	H	Image Reference Databases will include accurate,	L	

	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.				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 group 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 and this information is published on the SWP/GWP websites under the privacy notice section		

	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	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.	L	
	Where the force has not completed an appropriate policy document there is a risk that it will be in breach of section 42 of the Data Protection Act 2018 resulting in potential regulatory enforcement action and/or financial penalties	L	M	M	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	L	
	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	OIFR SOPS stipulate grounds and reasons for use of OIFR, ensuring consistency and oversight for each use. This includes that Operators must be lawfully present on premises before undertaking any OIFR comparison. Officers receive specific training on the extent of	L	

					searching with reference to selection of Image Reference Databases and also in searching Police systems on the return of a possible match to ensure that any data accessed is proportionate to the policing purpose for which the search is being conducted.		
	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	H	As part of OIFR training appropriate data protection training will be provided	L	
	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 adequate protection when handled and potential loss and damage	L	H	M	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.	L	
	As a result of technical failure there is a risk that the equipment will not function correctly resulting in incorrect returns or failure to	L	H	M	Officers/Staff involved in the pilot operational use of OIFR do not have	L	

	identify Possible Matches resulting in potential damage and distress or threat risk and harm to others				ready access to the complete Image Reference Databases. Operators and are briefed in respect of Image Reference Database 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. Those with roles specific to the oversight, operational use or management of OIFR systems or record management databases. 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		
	If multiple individuals are captured in the when an operator attempts to take a picture of the subject, there is a risk their personal information will be processed during the image capture leading to excessive and unnecessary processing	L	L	L	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 will be reviewed by the FRT and Biometrics Board and the SRO. This will help ensure that any future OIFR use will reflect learning	L	

					identified and that the use of OIFR remains an effective and proportionate policing tool 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. The OIFR App also has a 'cropping tool' that allows the Operator to limit the area of the Probe image only to the face of the subject and disregard any persons in the background of the image		
	There is a risk that processing of personal information of children and vulnerable persons will take place in the absence of parent or guardian which may lead to distress for the individual resulting in harm, complaints and enforcement action	M	H	H	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	L	

					similar manner to the way which Body Worn Video or a name check of that Subject is currently undertaken. The process will be explained at the time.		
	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	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.	L	
	Use of OIFR in where Operators are not lawfully present and conducting Police duties may lead to unlawful processing, reputational harm or legal challenge	M	H	H	Officers must meet the behaviours set out in the Code of Ethics. Any use of OIFR is auditable and recorded.	L	
	There is a risk that the algorithm contains bias leading to discriminatory identification of individuals from particular groups resulting in incorrect identification or lack of identification leading to	M	H	H	During the trial, the Facial Recognition Project team will monitor use of the OIFR app to identify Similarity scores	L	

	ethical issues, discrimination, reputational damage, unrest, loss of trust and confidence, increased harm to the public, complaints and enforcement action.				returned on matches, where 'no matches' occur what Similarity Scores are returned and identifying environmental conditions that result in inconsistent returns. The Threshold has currently been set based on the National Physical Laboratory guidance and also with experience of using Retrospective Facial Recognition (outside of the scope of this DPIA) to consider Similarity Scores that return correct matches and factors that impact those Similarity Scores. The use of body worn video will allow the project team to assess the circumstances OIFR was being used in to determine if failures are occurring as a result of poor use of the technology, failure to control environmental conditions (where possible) to obtain the best image or		

					failure of the algorithm to make correct identifications.		
	There is a risk that the capability of OIFR is used for non-policing purposes and function creep such as covert tactics leading to unlawful processing resulting in complaints, loss of trust and confidence, enforcement action	H	H	H	An audit trail is maintained to monitor use and prevent function creep. OIFR has been specifically designed to prevent this occurring. OIFR needs to be used in a frontal position, in very close proximity to the Subject. For this reason, it would not be suitable for covert tactics.	L	
	There is a risk that subject images will be retained and used for intelligence purposes leading to unlawful processing resulting in enforcement action	L	H	M	The app is designed to automatically delete the image and biometric template.	L	
R10 **IT Health Check** (where an ITHC has been undertaken and the overall level of risk has been identified							

Step 6: Sign off and record outcomes

Action	Name, position, date	Notes
Measures approved by:	Inspector Ben Gwyer 5369 Project Lead 19/11/2024	Actions must be integrated back into the project plan with completion dates and action owners.
Residual Risks approved by	Inspector Ben Gwyer 5369 Project Lead 19/11/2024	If accepting residual high risks, refer to DPO to consider ICO consultation before proceeding. Risks should be carried over to local risk registers when processing becomes business as usual.
DPO advice provided	Louise Voisey Data Protection Officer 19/11/2024	DPO to advise on compliance, mitigating measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	Accepted by Assistant Chief Constable Trudi Meyrick 13/01/2025	If overruled, an explanation must be provided.
Comments:		
Consultation responses reviewed by:	Inspector Ben Gwyer 5369 Project Lead 19/11/2024	If the decision does not align with the views of the consultees please explain
Comments:		

Force Information Security advice:	Geraint Morgan *Force Information Security Officer* *19/11/2024*	FISO to advise on security risks, mitigating measures and whether processing can proceed
FISO advice accepted or overruled by:		If overruled an explanation must be provided

This is a living document and must be updated where any changes to the details provided occur.

Annex A - Statement of Information Assurance Requirements for External Cloud Services Provider

The following table details the security considerations that should be considered as part of the process for procuring cloud services. Whilst all may not be applicable, they should at least be considered and comments should be made as to why they were not considered applicable.

1. Security Requirements

Access to the system and the data needs to be understood. If the following are required, appropriate access controls must be in place. Details should be given as to the type of controls:

Mandatory, Desirable	Requirement	Comments
M	**System administrator** This level must allow full access to the system, being able to undertake any part of the application including system setup. Please state both your admin access and your customer's (our) admin access. This should include identity and authentication controls. (NSCS Cloud Security Principle 10/12)	
M	**Nominated user** This must be a generic user with access to all major functionality, but no access to system setup. The system administrator should be able to monitor all activity generated by this user. This should include identity and authentication controls. (NSCS Cloud Security Principle 10/3)	

Mandatory, Desirable	Requirement	Comments
M	**User defined** This could be a user with specific rights as deemed fit by the system administrator. (NSCS Cloud Security Principle 10/3)	

2. Further security considerations

M	**Compliance with HMG Security Policy Framework (SPF), ISO / IEC 27001/Cyber Essentials Plus** If ISO compliant, give details as to what areas are compliant. Provide copies of all relevant current certifications. (NSCS Cloud Security Principle 4)	
M	**Information Security Policy** Please include a copy of your existing security policy document(s). (NSCS Cloud Security Principle 4)	
M	**Patching and system updates** The supplier must describe its current patching and updates processes for its IT systems, including patching frequency for both routine and critical patches. (NSCS Cloud Security Principle 5)	
M	**Data Protection Act 2018** How do you comply with the Data Protection Act 2018 (including GDPR) and uphold the eight principles of good practice. (NSCS Cloud Security Principle 4)	

M	**Physical, Procedural, Personnel and Technical Security Measures** The supplier must ensure there is adequate physical, procedural, personnel and technical security controls in place to prevent unauthorised access and dissemination of information assets. Please provide appropriate documentation that evidences this (such as Statement of Intent). (NSCS Cloud Security Principle 4)	
M	**Equipment Siting and Protection and storage** Please describe the location of any hosted environment and the virtual infrastructure. Include the hardware specification, operating software and number of shared services. If a cloud based service it must comply with Police Approved Security Facility (PASF) (NSCS Cloud Security Principle 2)	
M	**Data at rest and data in transit** Please provide details on how you would protect data both at rest and in transit, including the level of encryption that would be deployed. (NSCS Cloud Security Principle 1/2)	
M	**Screening** The supplier must apply the requirements of the Baseline Personnel Security Standard (BPSS) to all personnel (incl. third party contractors) prior to giving system access to assets holding police data. (NSCS Cloud Security Principle 6)	

D	**Independent review of Information Security** Do you have your site/service independently tested or audited? If so, please give details. The force will reserve the rights to perform an IT Security Assessment/audit at any time.	
M	**Control against malicious code** The supplier must ensure there are appropriate policies to manage risks from malicious code according to the impact level of the system/data which are developed and implemented. Please describe what is in place to mitigate this risk. (NSCS Cloud Security Principle 5)	
M	**Operational security** The supplier must have the process to manage the service securely such as to impede, detect or prevent attacks. This should include configuration and change management, vulnerability management, a form of protective monitoring. (NSCS Cloud Security Principle 5)	
M	**Segregation in networks** There must be adequate network segregation between the police information assets and third party assets – this can be physical or virtual. Please provide details of the segregation in place (computer, storage and networking components). (NSCS Cloud Security Principle 3)	

M	**External interfaces** The supplier must provide a clear overview (diagram/description) of the information flows, which must include external interfaces (physical and logical) and how access to customer data is controlled. (NSCS Cloud Security Principle 11)	
M	**Backup data** Backup data must be kept in secure storage and location that is physically separate from the system being backed up and to which access is strictly controlled. Mirrored systems should be fully tested on an annual basis to ensure that full data sets can be restored, applications can be accessed and that failover routines are effective. (NSCS Cloud Security Principle 2)	
M	**Adequate logging of access and activity, and appropriate protection of log data** Appropriate logging and auditing must be in place and that this data must be secured in such a way that tampering would be evident, for example by using the check-sum algorithm. Audit logs should be kept securely for a minimum of 12 months. (NSCS Cloud Security Principle 13)	

M	**Penetration Testing** To help provide assurances about the robustness of the system/service being procured, evidence should be given of any pentation testing that has been undertaken. It should also be expected that the force will conduct independent penetration testing of the system/service being procured prior to being accepted into service. If, as a result of this testing, vulnerabilities are identified by the pen-testing company, appropriate mitigation must be applied to the system/service provide, at their own expense, prior to implementation.	
M	**Reporting Information Security Events** A robust incident management system must be in place and all relevant information security incidents must be reported to the force Information Security Team within 24 hours. (NSCS Cloud Security Principle 5)	
M	**Secure disposal or re-use of equipment by supplier** When no longer required for its original purpose equipment containing sensitive information must be stored securely until it can be disposed of in line with current government guidelines and as agreed by the force. (NSCS Cloud Security Principle 2)	

3. Support and Maintenance

It should be made clear how the system/service will be supported, including whether the support will be remote or onsite.

Mandatory Desirable	Requirement	Comments
M	**Faults rectification** Detail how support is provided. If remote, how is that expected to be achieved and what security controls are in place to protect Force data? (NSCS Cloud Security Principle 9)	
D	**Upgrading** State the policy towards upgrading and implementing new software, including the frequency of any upgrades. This should include details of how upgrades are implemented (i.e. notice given to customer and whether it is at cost?) and whether they are mandatory to stay in support. (NSCS Cloud Security Principle 7)	
D	**Secure Development** Describe how the service development (upgrades) manages new and evolving threats. (NSCS Cloud Security Principle 7)	
M	**Supply Chain** Describe support provided by your 3rd parties and how supply chain security is managed (NSCS Cloud Security Principle 8)	

Mandatory Desirable	Requirement	Comments
D	**Secure use of the Service** Will clear guidance be given on how the customer (the force) is expected to use the service to maintain the secure controls in place (i.e. education of users, recommended configuration etc)? (NSCS Cloud Security Principle 14)	

4. Back up and resilience

Appropriate description and evidence should be given on how the system/service will protect Force data should it be subject to a major failure. This should include details on how CIA will be maintained.

Mandatory Desirable	Requirement	Comments
M	**Business Continuity** Give details of your Business Continuity Plan (BCP), including how system/service continuity will be maintained in the event of a major failure. (NSCS Cloud Security Principle 2)	
M	**Protecting the data** The system/service must have full back-up and restore capabilities in the event of recovery from hardware or software failure. (NSCS Cloud Security Principle 2)	

5. Data Retention and Disposal

As part of the information life cycle, consideration should be given on how long the data will be held and how it will be disposed of once the contract expires.

Mandatory Desirable	Requirement	Comments
M	**Archiving (if required)** The supplier must state whether there is the ability to archive after a specified period and whether this is an automated process. Please state if this is an additional cost. (NSCS Cloud Security Principle 2)	
M	**Data retention** The system/service must support the Forces' requirement to adhere to the Management of Police Information (MOPI) and relevant Legislation/regulations (such as Data Protection Act and GDPR). Explain the proposed data retention policy that will be in place.	
M	**End of life strategy** Please give details of what happens to Force data once the contract has ended (i.e. deletion or returned to owner?). Data returned must be in a format agreed by the force. Details should include any transitory arrangements that might be put in place, along with a costing model.	
Name		
Position		
Company		

Date		**Telephone**		**Email**	

DPIA Ref:2 45
Police Force: Joint SWP/GWP

Annex B Risk Assessment Matrix

Risk Matrix	Likelihood	Rare	Unlikely	Possibly	Likely	Almost Certain
Impact	Multiplier	1	2	3	4	5
Insignificant	1	1	2	3	4	5
Minor	2	2	4	6	8	10
Moderate	3	3	6	9	12	15
Major	4	4	8	12	16	20
Critical	5	5	10	15	20	25

Recording in Step 5

Low (L) 1-4
Medium (M) 5-12
High (H) 15-25

Impact Definitions Table		Value				
		1	2	3	4	5
EXPLANATION	**Impact on reputation**	Likely to reduce an individual citizen's perception of SWP	Likely to reduce the perception of SWP by many citizens	Likely to result in undermined confidence in SWP at a regional level. Regional press involvement	Likely to result in undermined confidence in SWP at a national level. National press involvement	May lead to a complete breakdown in public trust. Ministerial involvement
	Impact on privacy and identity	Loss of control of a single persons data would cause inconvenience to them	Loss of control of many citizens' personal data beyond those authorised by each. Possible requirement to report to ICO	Loss of control of a citizen's sensitive data. A compromise to the identity or financial status of an individual. Possible enforcement action by ICO	Loss of control of many citizens' sensitive or financially significant personal data. Compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack Possible fine by ICO up to £0.5m	Widespread compromise of identity management systems or financial systems across SWP. Prosecution by ICO and report to Parliament
	Impact on life and safety	Inconvenience or cause discomfort to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individuals safety or liberty.	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
	Impact on provision of emergency services	Minor disruption to service activities that requires reprioritisation at the local level to meet expected levels of service	Minor disruption to emergency service activities that requires reprioritisation at the area or divisional level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the county or organisational level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the national level (e.g. one police force requesting help from another) to meet expected levels of service	Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency services) to meet expected levels of service
	Impact on crime fighting	Hinder the detection, impede the investigation, or facilitate the commission of low-level crime (i.e. crime not defined in legislation as "serious crime"), or hinder the detection of serious crime	Hinder the detection, impede the investigation, or facilitate the commission of a crime (defined in legislation)	Impede the investigation of, or facilitate the commission of serious crime (as defined in legislation)	Cause major, long-term impairment to the ability to investigate serious crime (as defined in legislation)	Cause major, long-term impairment to the ability to investigate serious organised crime (as defined in legislation).

	Impact on judicial proceedings	Minor failure in local Magistrates courts	Cause a low-level criminal prosecution to collapse; cause a conviction for a low- level criminal offence to be declared unsafe or referred for appeal.	Cause a serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred for appeal	Cause a number of criminal convictions to be declared unsafe or referred to appeal (e.g. through persistent and undetected compromise of an evidence-handling system)	Major long-term damage to UK judicial system