STANDARD OPERATING PROCEDURES FOR THE OVERT USE OF OPERATOR INITIATED FACIAL RECOGNITION (OIFR)

Protective marking:	Official
Publication scheme Y/N:	No
Title:	Standard Operating Procedure for the overt use of Operator Initiated Facial Recognition (OIFR)
Version:	Version 1.3
Summary:	Establishes procedures for the use of OIFR as a policing tactic during the OIFR Pilot
Department:	Digital Services Division
Review date:	14/12/2025

Version	Date	Authority	Evidence of approval	Record of change
0.1	28.07.2021	Project Lead	Ch. Insp Scott Lloyd	Initial Draft
0.2	29.07.2021	Project Lead	Ch. Insp Scott Lloyd	Minor amendments
0.3	17.08.2021	Project Lead	Ch. Insp Scott Lloyd	Minor Amendments
0.4	20.09.2021	Project lead	Ch Insp. Scott Lloyd	National terminology
0.5	03.11.2021	FRT Board	Governance Review	No Amendments
0.6	25.01.2022	DSD Lead	Ch Supt Simon Belcher	Pilot Sign Off. No Amendments
1.0	19.06.2024	Project Lead	Inspector Ben Gwyer	Amendments to include NPL Findings
1.1	14.12.2024	Project Lead	Inspector Ben Gwyer	Final scrutiny amendments

Contents

Terms & Definitions: Capitalised terms used within this OIFR SOP shall have the meaning given to them in section 3 of OIFR Policy Document unless otherwise defined.

1 Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted by South Wales Police (SWP) / Gwent Police (GWP) personnel using the OIFR in support of the policing tactic. Compliance with the SOP will help ensure a corporate response to the use of this policing tool.

1.2 The driving force behind the development of OIFR is to ensure front line operational police officers and Police Staff have access to accurate information and intelligence, so that they can effectively navigate the National Decision-Making Model (NDM) and ultimately make the best decisions possible.

1.3 OIFR will be available to officers through their SWP/GWP issued mobile phone as part of the existing iPatrol application.

1.4 OIFR enables the Operator to acquire an image of a Subject and probe this image in near real time against an Image Reference Database(s) of existing known Candidate Images to assist in their identification for a policing purpose.

1.5 OIFR has been developed to integrate with existing features contained within iPatrol including Niche RMS, Police National Computer, warrants management system and the Electronic Pocket NoteBook (ePNB).

2 Application

2.1 All SWP/GWP officers and police staff, including the extended police family and those working voluntarily or under contract to the Commissioner must be aware of, and are required to comply with, all relevant SWP/GWP policy and associated procedures.

2.2 This SOP applies in particular to officers and staff in the following roles: -

a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the use of OIFR; and

b) All police officers and police staff involved in any subsequent investigation resulting from the operational use of OIFR; and

c) OIFR development team.

Note: This list is not intended to be exhaustive.

3 Terminology

3.1 This SOP focuses exclusively on OIFR. Terminology relating to OIFR is defined in the SWP/GWP OIFR Policy Document.

4 Authority to use OIFR

4.1 The authority to use OIFR as a policing tactic is supported by the Senior Responsible Officer (SRO).

4.2 Prior to use of OIFR the Police and Crime Commissioner for the SWP area and the Police and Crime Commissioner for the GWP area have been engaged in its development and potential use.

5 When and Where OIFR can be used

5.1 OIFR should not be used to replace traditional or less intrusive means of identification, such as having a conversation with the individual who then provides their name which is checked against police indices to identify them. Wherever possible, OIFR should only be used after an interaction has occurred between the Operator and the Subject. An example where an engagement could not occur beforehand would be a deceased person or a person who is unconscious.

5.2 OIFR does not replace the existing SWP/GWP Retrospective Facial Recognition (RFR) process. OIFR must not be used to attempt to identify any person from a computer screen or other such image. RFR has its own suite of supporting policy documents that are available via the SWP/ GWP facial recognition website so are not in the scope of this document.

5.3 Use of OIFR will only occur when the identity of a Subject is not known and at least one of the **reasons** and at least one of the **grounds** for use is present.

5.4 Reasons for use: -

a. The Subject is unable to provide their details
b. The Subject has refused to provide their details.
c. It is reasonable suspected the Subject has provided false details.

5.5 **'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.

5.6 OIFR may be used for all the listed grounds in public places and in private places where Operators are lawfully present for a policing purpose.

5.7 Grounds for use : -

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.

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.

d. 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**.**

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

5.8 **'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.

5.9 '**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.

5.10 **'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.'

Officers Note

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

- supporting the identification and arrest of people wanted for criminal offences
- supporting the identification of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc)

5.11 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 and the Code of Ethics.

5.12 Force must not be used to obtain a Probe Image with OIFR use. Identification by OIFR would not be deemed a justification to use force for a policing purpose.

5.13 Body worn video (BWV) will be used to record the use of OIFR for audit purposes. BWV will be categorised on the appropriate evidence management system in line with 'stop search' and 'use of force' policy.

5.14 When OIFR is used, it is for the Operator to make all reasonable, less intrusive enquiries, to identify of the Subject prior to using OIFR. The Operator should document these enquiries in the circumstances section of the OIFR as justification for the necessity to use OIFR.

5.15 If a Subject cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, or any action taken, and have a lawful basis for doing so.

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

5.17 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 a person. However, the officer 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 could 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

5.18 Operators do not require consent from the Subject for the purposes of obtaining an image for the purposes of OIFR. Operators do however require a level of co-operation from the Subject, staying still and not taking action to obscure their face. If the Subject refuses to co-operate for the purposes of obtaining an image, the Operator will need to consider the proportionality of other policing tactics available to them and to justify any action that they then undertake.

Protest/ Demonstrations and Densely Populated Areas

5.19 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.

5.20 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".

5.21 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.

5.22 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 should be captured on BWV and recorded in the ePNB of the Operator as additional information through the OIFR app.

6 Providing the Subject with Information

6.1 This section covers what information must be provided to the Subject during and post OIFR.

6.2 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.

6.3 The Operator must record any concerns raised by the Subject relating to the use of OIFR within the circumstances free text field.

6.4 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.

6.5 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

6.6 When OIFR is utilised, the Operator must ensure they do so lawfully, and in an appropriate and proportionate manner. Operators must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject to OIFR, should be supplied with an OIFR information leaflet or directed towards the SWP/GWP Facial recognition website and privacy notice for further information.

6.7 Any person who requires additional information relating to OIFR should be provided with contact information for the SWP/GWP Facial Recognition Team:

FRT@South-Wales.police.uk

Children and Vulnerable People

In some cases, it will be deemed necessary to utilise OIFR to identify children or vulnerable individuals.

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

6.8 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.

6.9 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.

6.10 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

This list is not exhaustive but reflects options that are reasonably available and should be considered.

Welfare and Safeguarding of Children and Vulnerable People

6.11 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).

6.12 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.

6.13 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.

6.14 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.

7 How to use OIFR

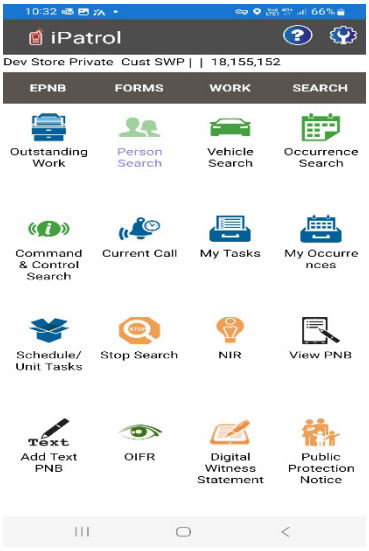
Launching the OIFR app

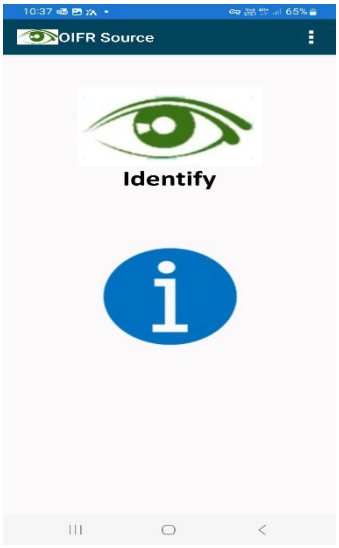
7.1 Access to the OIFR app is only granted following satisfactory completion of the training provided.

7.2 OIFR is accessed via the existing iPatrol Application on the Samsung mobile device.

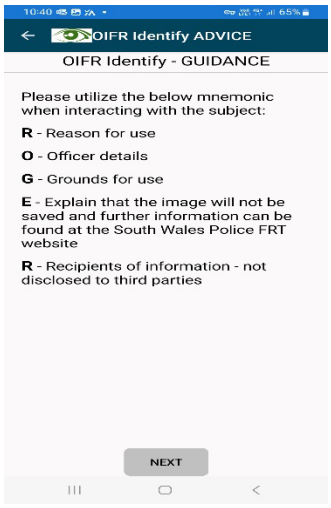
7.3 On installation, the OIFR logo features on the iPatrol home screen. iPatrol features four headers:

7.3 OIFR is contained within the SEARCH header as a function icon. *(Below Left*) Once selected and launched, the Operator is presented with 2 large icons, which detail the functions contained within the OIFR app. *(Below Right)*





7.4 To search using OIFR, select the IDENTIFY icon. A guidance screen will then be displayed. This will be shown every time OIFR is used and provides a guide to effective operation and a reminder of legal powers. *(Below)*



Choosing Reason/Grounds/Image Reference Database(s)/Location of Search

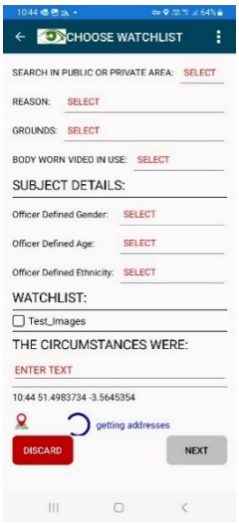
7.5 On pressing the 'NEXT' button, the OIFR app will then progress to the search phase. This will prompt the Operator to select:

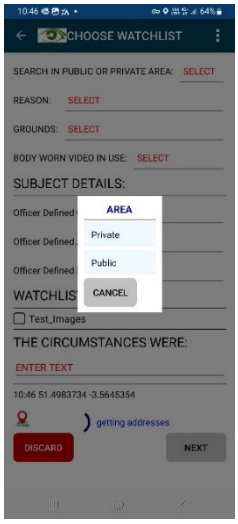
1. whether the search is being conducted in a public or private place
2. the reason and grounds for use
3. an Image Reference Database(s) to conduct the comparison against
4. whether BWV is being utilised (and if not, why not)
5. the officer defined gender of the subject, age of the subject and ethnicity of the Subject,

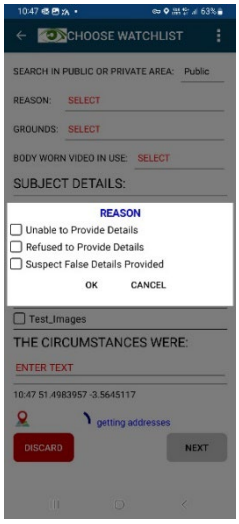
There are text fields to record:

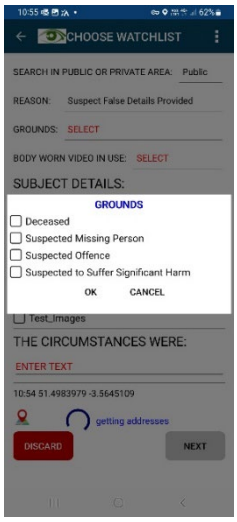
6. the circumstances giving rise to the grounds and reason for the search,
7. the location of the search. As with other iPatrol functions, this will automatically populate with the GPS location as recorded by the SWP/GWP issued mobile phone. If the GPS Location is not found, a freetext box is provided requiring the Operator to manually enter the location.

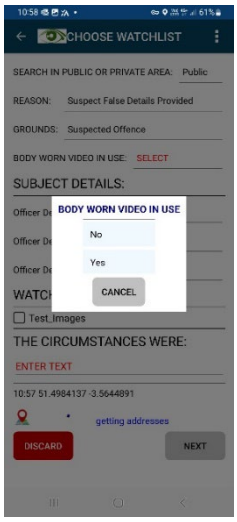
The above are mandatory fields and the Operator will not be able to progress without completing these fields.







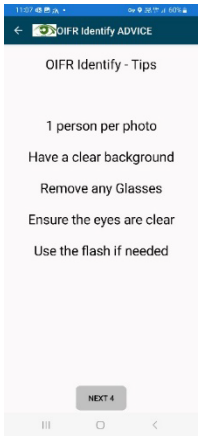




7.6 Once the selections have been made and the circumstances have been recorded, the OIFR app will then move to the image capture screen for the Operator to capture an image to be searched against the chosen Image Reference Database(s).

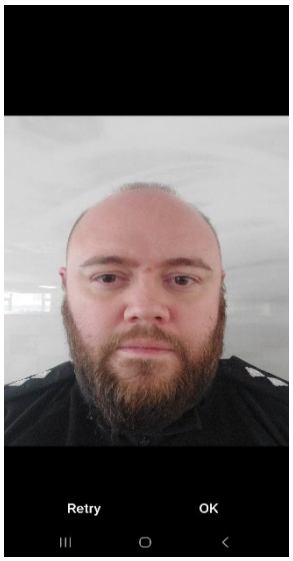
Obtaining a Probe Image

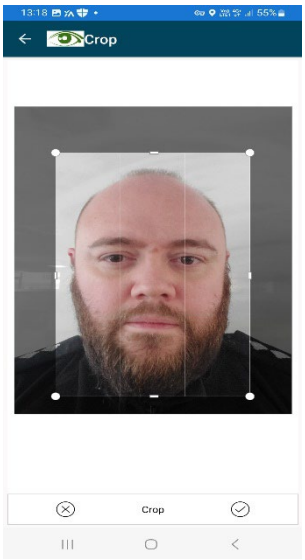
7.7 After completing the mandatory fields as above, the Operator will be shown the below 'Top Tips' page, offering guidance on obtaining the best image possible and minimising the impact of environmental, subject and system factors that may impact the OIFR app's ability to recognise the Subject's face.



7.8 The OIFR app has been configured to ensure any image captured via the mobile phone camera through the OIFR app remains within OIFR. The image cannot be saved within the phone to any other location. Once the search is completed, the 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) are available to the Operator.

7.9 Once an image has been captured, it will be presented to the Operator to ensure it is of sufficient quality for comparison (no blurriness, glare or poor lighting). A 'retry' option is provided, for use if the Probe Image obtained is unsuitable however on selection of 'retry', the previous image is deleted *(Below left).* 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 (*Below right*).



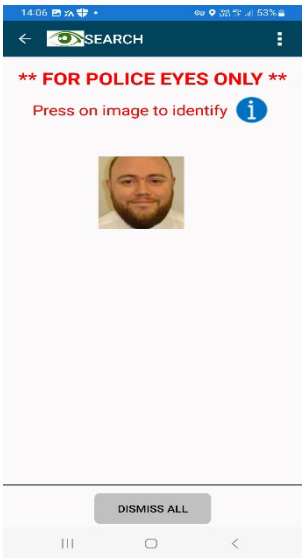


7.10 When the Operator has obtained a suitable image, selecting the 'SEARCH' option will initiate the comparison process, searching against the selected Image Reference Database(s) on the previous page.

7.11 The OIFR Probe Image is not retained within the OIFR app, the SWP/GWP mobile phone, or in the iPatrol application.

Results

7.12 The results returned will be the Candidate Images with Similarity Scores exceeding the Threshold Setting. Up to six images scoring above the Threshold setting can be returned for consideration by the Operator. 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'. Only images from the selected Image Reference Database(s) will be returned. *(Below)*



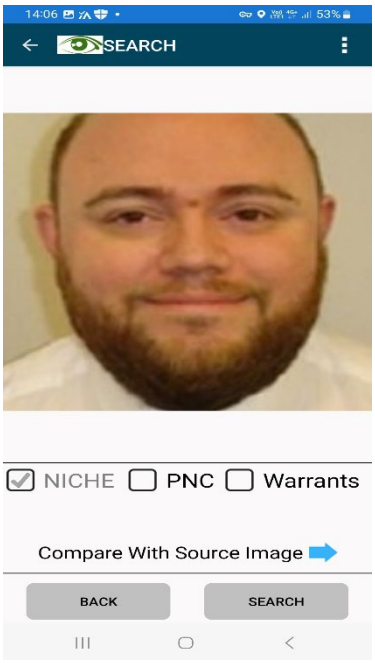
7.13 It is for the Operator to decide whether the Candidate Image(s) returned is recognisable as the Subject. The search will only return the top six Candidate Images with Similarity Scores exceeding the Threshold Setting. At this stage, no name or other personal information is presented to the Operator.

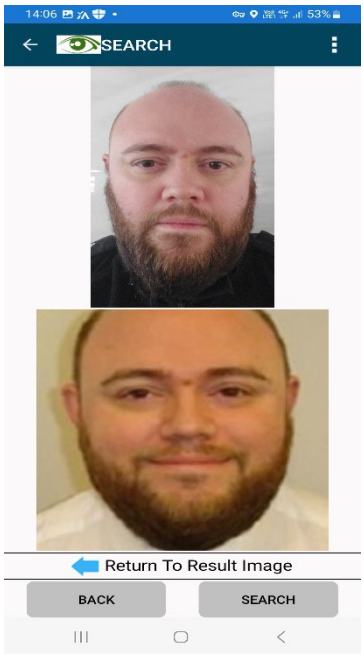
7.14 If searching against the custody Image Reference Database, it is important to note that there may be multiple Candidate Images of the same person returned to the Operator. This is because the custody Image Reference Database contains separate images from each previous detention for any person included.

Searching within Candidate Images

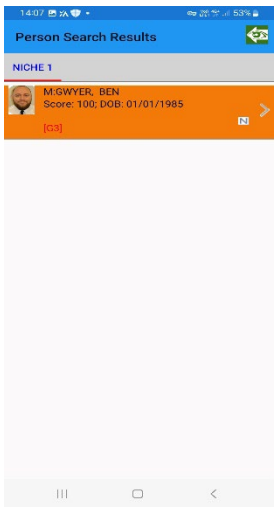
7.15 If the Operator believes a Candidate Image to be a Possible Match, the Operator is able to search for further details by tapping on the Candidate Image. This will then generate a search screen allowing the Operator to select the police systems to be searched *(Below left).* The systems to be searched will be determined by the Operator's policing purpose and it will be the responsibility of the Operator to ensure the proportionality of the searches against the identified systems.

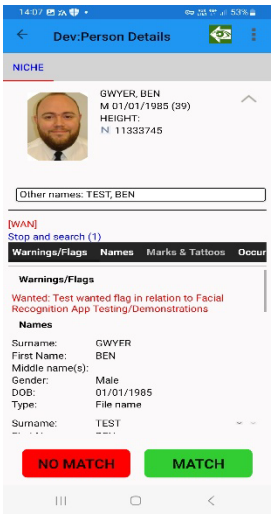
7.16 Before the search occurs, the Operator is also available to compare the Probe and Candidate Image. (Below right)





7.17 The OIFR app will present the standard iPatrol search function and will allow the Operator to navigate through Niche records, or other identified police record systems, in the usual way. *(Below)*





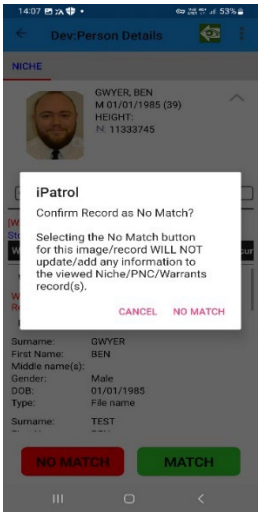
Auditability

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

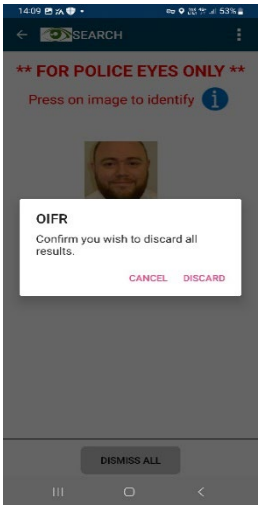
7.19 This takes the form of two buttons ‘NO MATCH’ and ‘MATCH’ which feature at the bottom of the Person Details screen. Selection of one of these buttons is mandatory to record the outcome of any search performed as a result of OIFR.

No Match

7.20 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 *(Below).* This will return the Operator to the original Candidate Images however with the previously chosen Candidate Image now greyed out.



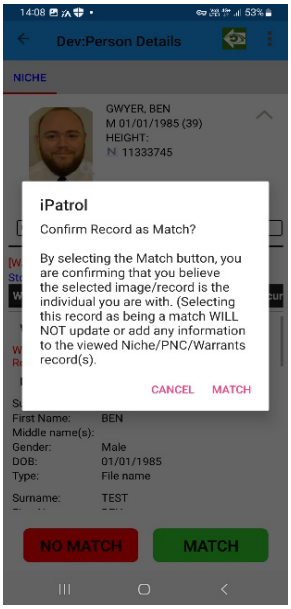
7.21 If the Operator determines that none of the Candidate Images returned matches the Subject, the Operator should select ‘DISMISS ALL’. *(Below left)* The user is then asked to confirm that they wish to discard all results. At this point, the Probe Image will no longer be accessible for further searches 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.



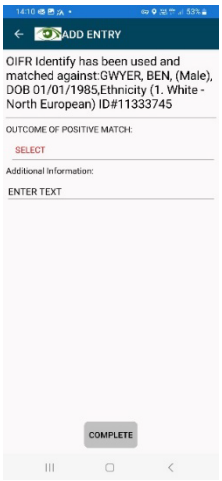
7.22 An ‘additional information’ free text box is presented for Operators to capture any other information relevant to the OIFR search. The Operator presses ‘COMPLETE’ at the bottom on the screen, the use of the OIFR app is now concluded.

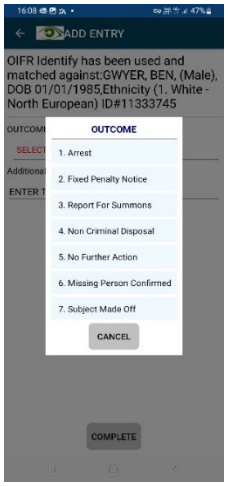
Match

7.23 If the Operator selects the ‘MATCH’ option referred to in 7.19, the Operator is presented with a confirmation selection to confirm that the Operator believes a match has been made. If this has been selected in error, the Operator has the opportunity to ‘cancel’ the ‘match’.



7.24 If 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 pressing '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. *(Below left)* This presents a drop-down list with possible outcomes for the Operator to select and document. (*Below right*)



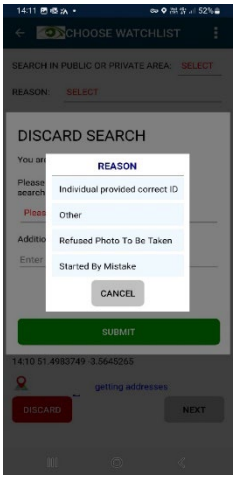


7.25 Upon selecting an outcome, the Operator selects 'Complete' and the use of the OIFR app is concluded.

Further information

7.26 For both matched and non-matched images the Operator 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.

7.27 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. 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).



Automatic Auditability – ePNB Ingestion

7.28 Effective auditing and accountability with regard to use of OIFR is of paramount importance, ensuring transparency and maintaining public confidence. In light of this, any use of the OIFR app automatically generates an audit log which is recorded in the Operator's ePNB. The Operator has no means to edit, 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.

7.29 **A. OIFR Search initiated**

This entry automatically inserts into the ePNB of the Operator as soon the OIFR app is started. At this point, the Operator has not recorded any information and no images have been obtained. This entry is time and date stamped and the entry reads:

02/02/ 2024 15:56	OIFR Search Initiated 02/02/2024 15:56:41 OIFR SEARCH INITIATED

7.30 **B. OIFR Identify Search**

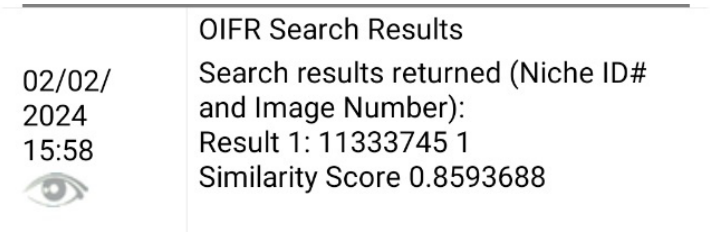
This entry captures the data input by the Operator and includes:

- location the GPS location (or manual entry if GPS is not available)
- whether the search has been conducted in a public or private place
- the reason for the search, the grounds for the search
- whether Body Worn Video (BWV) was used (and if not, why BWV was not used)
- the Officer identified gender of the Subject,
- the Officer identified age group of the Subject
- the Officer identified ethnicity of the Subject
- the Image Reference Database(s) that the OIFR Comparison that has been conducted against

02/02/ 2024 15:57	OIFR Identify Search Image from Camera Location: HQ Search Area: Public Reason: Suspect False Details Provided Grounds: Suspected Offence Body worn video in use: Yes If no, why: Gender: Male Age: 31 - 60 Ethnicity: 1. White North European OIFR Identity Search Commenced Watchlist(s) searched against Test_Images

7.31 **C. OIFR Search Results**

This entry records how many results were returned (up to a maximum of 6), their unique Niche identifier, their position (Result 1, Result 2 etc), and the Similarity Score that each Candidate Image returned.

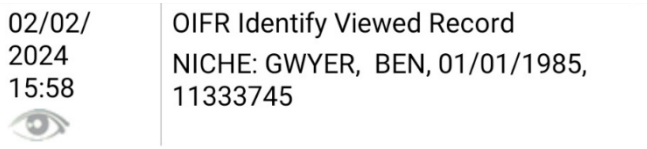


7.32 **D. OIFR Identify Record Viewed**

This additional entry will record the Operator's selection of a Candidate Image and subsequent search of Niche.

This entry will also record if any other Police systems are searched, e.g., PNC or warrants management system

If multiple Candidate Images are searched, then multiple records will be created to reflect this.

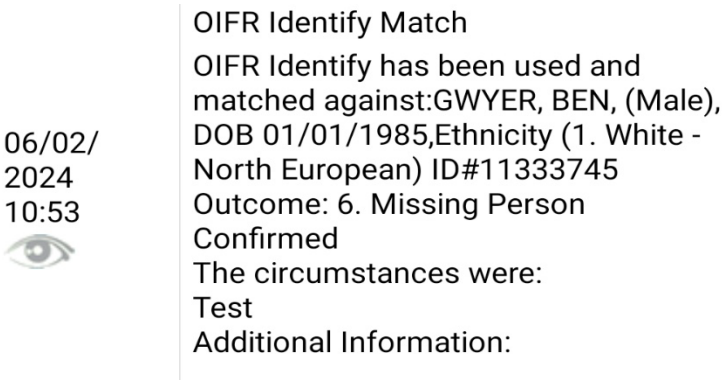


7.33 **E. OIFR Identify Match**

This entry is created if the "Match" option is chosen. The ePNB log will record the circumstances and monitoring information of the Subject.

The outcome shown is selected from a pre-defined drop-down menu.

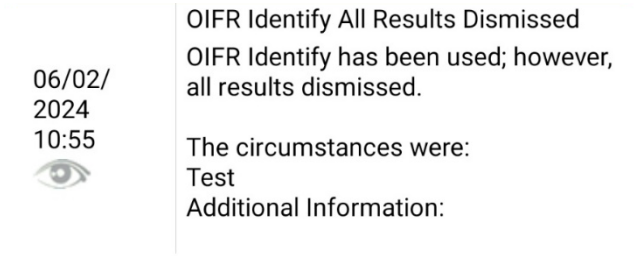
A free text field, in which the Operator is to record any other useful information to include any concerns raised during OIFR use.



7.34 **F. OIFR Identify No Match**

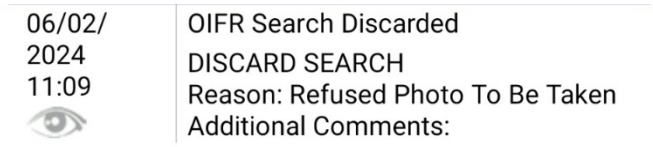
This entry is created if the “No Match” option is chosen. As above this entry reflects Operator input.

A free text field, in which the Operator is to record any other useful information to include any concerns raised during OIFR use



7.35 **G. OIFR Search Discarded**

If the Operator abandons the search at any point prior to results being returned, the below entry will be documented. This will also include the input from the Operator as to the reasoning the OIFR Comparison has been abandoned.



7.36 The automated completion of ePNB entries provides an audit function that allows use of OIFR to be monitored and evaluated. The records contained within (E) and (F) above are consistent with the existing iPatrol Stop and Search audit requirements.

7.37 The ePNB entries are accessible by the Operator for review and also by the Operator’s Supervisor, Professional Standards Department and other Police Officers or Staff with oversight authority for the use of OIFR. SWP/ GWP will also have in place a Governance structure to ensure that supervision is thorough and robust in regard to utilisation of the OIFR app, utilisation of body worn video, completion of mandatory fields and ensuring satisfactory circumstances to justify use of OIFR, as well as allowing the capture and review of relevant data relating to demographic data of persons subject of OIFR.

8 Image Reference Database(s)

8.1 OIFR will utilise SWP/GWP custody images and SWP/GWP images of missing persons. Image Reference Databases will reside on the FRT System and not the Operator’s OIFR Device.

8.2 Image Reference Database(s) are made up of the entire custody database of SWP/GWP. It also includes live missing persons (deemed increased risk) for the SWP/GWP area.

8.3 The Image Reference Databases are a direct duplication of the images that are currently legitimately stored in Niche RMS, (SWP/ GWP criminal records management system) which is the source of custody images.

8.4 The Operator will actively select the Image Reference Database to be utilised, this can be one or both of the Image Reference Databases mentioned above depending on the necessity for use.

9 SWP/GWP OIFR Documents

9.1 Assessments; Prior to the use of OIFR, the following assessments need to be created, reviewed, and amended where necessary: -

(i) Data Protection Impact Assessment* (Review/Amend/Adopt); and

(ii) Equality Impact Assessment* (Review/Amend/Adopt).

Note: *Any assessment listed above showing `Review/Amend/Adopt' has already been created by the SWP/GWP FRT team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for OIFR use.

10 Management of Risk

10.1 Each use of OIFR should be risk assessed in line with SWP/GWP procedure. The anticipated risk to officers and the public should be balanced against the overall information and intelligence that is available at the time, relevant factors linked to persons included on the Image Reference Database(s) (e.g., seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the use, timing, community tension, and any other factors that appear relevant.

10.2 The level of resources, including back-up contingencies, required to support each use is a matter to be determined by the Operator.

10.3 Given the level of intrusion linked to the use of OIFR and the processing of biometric data, it is vital that the Operator is able to respond to a Match and to meet the law enforcement purpose for the use of OIFR.

10.4 All SWP/GWP officers using OIFR must be compliant and in date with SWP/GWP First Aid and Public and Personal Safety Training (PPST) requirements. All SWP/GWP officers and staff involved in the use of OIFR must receive OIFR training prior to use.

11 OIFR Operational Roles

OIFR Command Team

11.1 OIFR must be supported with a clear command structure. The following roles are defined for the purpose of creating an appropriate hierarchical command structure: -

a) Senior Responsible Officer (SRO) has strategic command of OIFR. The SRO will liaise as necessary with National Police Chief Council (NPCC) ranked officers and the South Wales Police and Crime Commissioner and the Gwent Police and Crime Commissioner. The SRO chairs the Facial Recognition Technology and Biometric Board which will review the performance outcomes of OIFR and tactical deployment of the technology.

b) The Divisional Commanders will have tactical command for the deployment of OIFR within their division. It will be their responsibility to ensure effective governance of the technology and accountability of the Officers deploying OIFR in their division. The information collated from these reviews will feed into force scrutiny boards.

c) The relevant Inspectors responsible for departments/ geographical areas will ensure that Supervisory checks are being made into the use by Operators on their teams to determine if the use is in line with policy and that all use is justified, proportionate and ethical.

d) The Digital Services Division FRT Project Lead will retain responsibility for policy and procedure relating to OIFR and will engage and support all levels of the Command structure in the review of OIFR usage and outcomes

Operator

11.2 The Operator is the Police Officer/ Police Staff Member operating OIFR, who is responsible for establishing the legal basis for using OIFR and adjudicating any Candidate Images returned for Possible Matches.

11.3 Operators receive detailed training to ensure an understanding of OIFR and the FRT System, how it performs, and what effect Subject, System, and Environmental Factors might have. This training and subsequent knowledge checks must be completed prior to being granted access to use OIFR operationally.

11.4 Should concerns become apparent regarding an Operator's use of OIFR, permission to use OIFR can be removed remotely until such time that the FRT Project Lead and SRO are satisfied that the concerns have been properly addressed.

11.5 The use of OIFR is to be used in an overt manner, however Officers may utilise OIFR in Uniform or on plain clothes duties. Where Officers are deployed on Plain clothes duties, they will be expected to make reasonable efforts to identify themselves to the Subject of the OIFR Search

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

11.7 The Operator must make their own final decision on whether a Match is made. In making their decisions, the Operator must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of returned Candidate Images.

11.8 When OIFR is used, it is for the Operators involved to investigate the identity of the person using appropriate and lawful means at their disposal.

11.9 Officers should always seek to make sufficient enquiries to satisfy themselves of their grounds to arrest, detain, or take any other Police action. Where confronted with a non-compliant Subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

11.10 Where members of the public choose to exercise their right to object to use of OIFR, Operators are reminded that this is not an offence. The police have no legal powers to compel members of the public to be subject to OIFR. None of this means that Operators, or other officers involved in an ancillary role, cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so.

12 OIFR System Security

12.1 OIFR is managed and deployed via a secure Application Management Console and is not available via any commercial application store or catalogue.

12.2 Once deployed to a device, that device is also subject to a rigorous security framework, password structure and certification process.

12.3 In order to access OIFR within the device, a connection will be made to the SWP server via a Virtual Private Network (VPN) which again is authenticated.

12.4 Image Reference Databases which are searched against are held on the FRT System which is single secure server to which the Operator has no access.

13 Data Retention & Data Management

13.1 SWP/GWP must ensure that the processing of any data associated with OIFR is conducted in a lawful way and in compliance with the SWP/GWP OIFR documents. This means that:

Particular to OIFR and FRT System

a) Image of the Subject as captured by OIFR (Probe Image) - immediately deleted in the OIFR Device and FRT System.

b) Biometric Template of Probe Image - immediately deleted in FRT System

c) Candidate images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS

Electronic Pocket Notebook

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

Source System – Custody Images

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

14 Contact Information

14.1 The SWP/GWP FRT team can be contacted using the following email address:

FRT@South-wales.police.uk.

15 Further Documentation

15.1 Further documentation is available providing useful information relevant to FRT. This is detailed below.

a) Information Management APP; www.app.college.police.uk/appcontent/information-management;

b) National Decision Model; www.app.college.police.uk/app-content/nationaldecision-model;

c) National Intelligence Management; www.app.college.police.uk/appcontent/intelligence-management;

d) College of Policing Code of Ethics; www.app.college.police.uk/code-ofethics;

e) Home Office Biometric Strategy – Published June 2018; www.gov.uk/government/publications/home-office-biometrics-strategy;

f) High Court Ruling – R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin); www.judiciary.uk/wpcontent/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.