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 0.6
Summary:	Establishes procedures for the use of OIFR as a policing tactic during the OIFR Pilot
Department:	Digital Services Division
Review date:	25/01/2022

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

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 have access to as much accurate information and intelligence as possible, 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 device (Samsung Galaxy XCover Pro Enterprise Edition) 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 images to assist in their identification for a policing purpose.

1.5 OIFR has been developed to integrate with existing features contained within iPatrol include Niche RMS, Police National Computer 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 SWP/GWP Police and Crime Commissioner 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 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 must only be used after an interaction has occurred between the Operator and the Subject.

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.

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 **grounds** for use is present.

5.4 Reasons for use: -

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

5.6 Grounds for use: -

Is suspected to be:

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

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

c. Missing persons deemed increased risk.

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

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

5.7 **'Further police action required'.** This term will reflect the nature of the criminal investigation underway. There 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.

5.8 '**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.

5.9 **Presenting a risk of harm'**. This term will reflect that using OIFR is necessary to manage the risk of harm identified and police action is required in order to manage the risk of harm.

Officers Note

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

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

5.10 Operators are reminded of the importance of effective tactical communication and that any action taken must be considered in line with the National Decision-Making Model.

5.11 Force may not be used to obtain a Probe Image with OIFR use based on the necessity to identify the Subject.

5.12 Body worn video will be used to record the use of OIFR for audit purposes.

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

5.14 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, any action taken, and have a lawful basis for doing so.

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

5.16 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 private place. Some places, and the people expected to be at some places by their nature attract greater privacy expectations than others.

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 possible the operator will inform the Subject that they intend to use OIFR and must provide details for the reason 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 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 OIFR information leaflet.

6.7 Any Subject, in the normal course of events, should also be offered further information about the technology. Any person who requires additional information relating to OIFR should be provided with contact information for the SWP/GWP FRT team (FRT@South-Wales.police.uk).

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

7 How to use OIFR

Launching OIFR

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

7.2 On installation, the FRApp logo features on the iPatrol home screen. iPatrol features four headers:

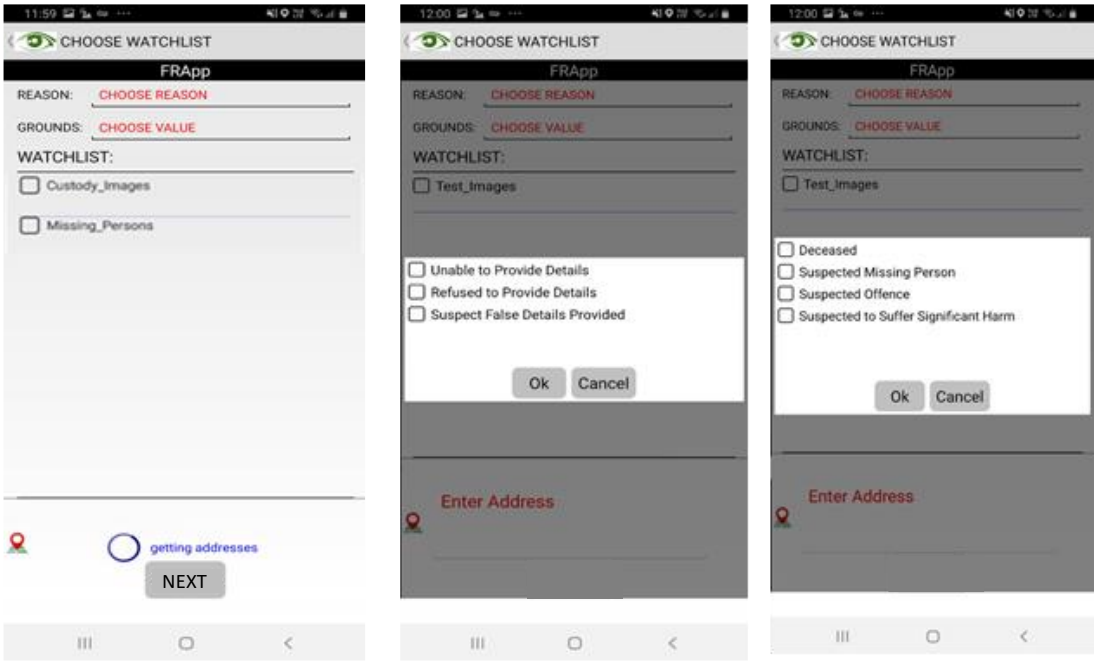
7.3 OIFR is contained within the SEARCH header as a function icon. *(Below Left*) Once selected and launched, the Operator is presented with 4 large icons, which detail the functions contained within the FRApp. *(Below Right)*

7.4 The LOCATE and ENROL functions have not yet been developed and do not currently operate.

7.5 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

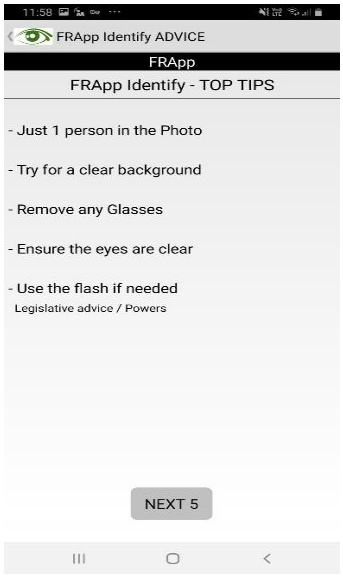
7.6 On pressing the NEXT button, OIFR will then progress to the search phase. This will prompt the Operator to select the reason and grounds for use, an Image Reference Database(s) and record the location of the search *(Below*). As with other iPatrol functions, if the GPS Location is not found, a freetext box is provided requiring the Operator to manually enter the location. *(Below)*



7.7 Once all three choices have been made OIFR will then allow the user to capture the image for OIFR to search against the chosen Image Reference Database(s).

Obtaining a Probe Image

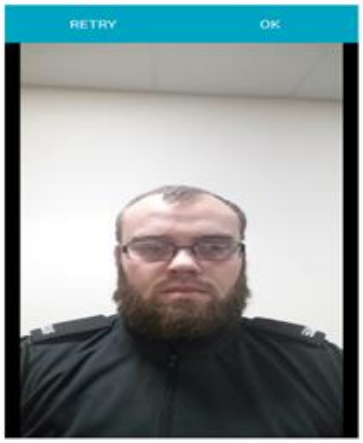
7.8 After selecting the Grounds, Reason, Image Referecne Database(s) and Location of the search, the user will be shown the below 'Top Tips' page, giving advice on how to obtain the best image possible to allow for OIFR to recognise a face.



7.9 The device camera has been configured to ensure the image remains within OIFR and is not saved or available for later retrieval.

7.10 A 'retry' option is provided, for use if the Probe Image obtained is unsuitable, for example blurred or obscured, however on selection of 'retry', the previous image is deleted. *(Below left)*

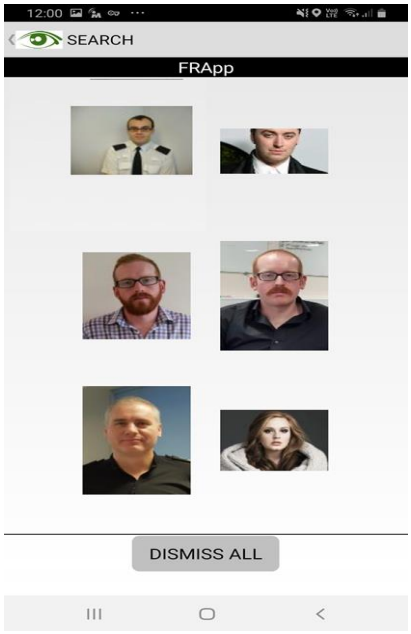
7.11 When the Operator has obtained a suitable image, selecting the SEARCH option will initiate the search process, against the Image Reference Database(s) selected on the previous page. (Below right)



7.12 The image which has been taken is not stored within the device or anywhere within the iPatrol application and upon pressing SEARCH, RETRY or CANCEL, the image is no longer retrievable.

Results

7.13 The results returned will be the Candidate Images that most closely match the Probe Image. Only images from the selected Image Reference Database(s) will be returned. *(Below)*



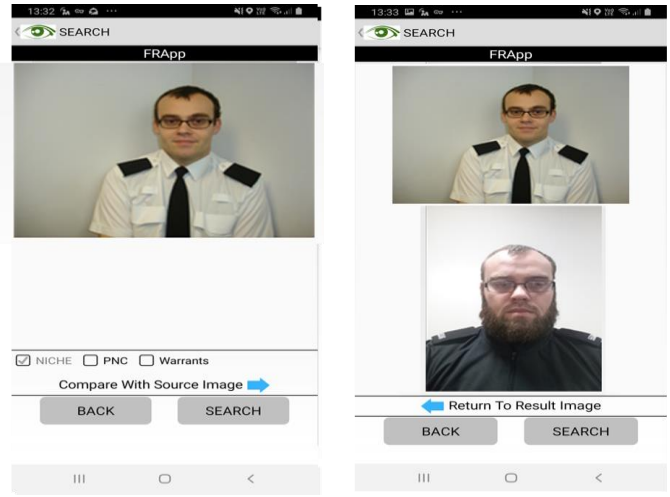
7.14 It is for the Operator to determine whether any of the six returned Candidate Image is recognisable as the Subject. The search will always return the top six similar Candidate Images even if the Subject's image is not contained within the chosen Image Reference Database. At this stage, no name or other personal information is presented to the Operator.

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

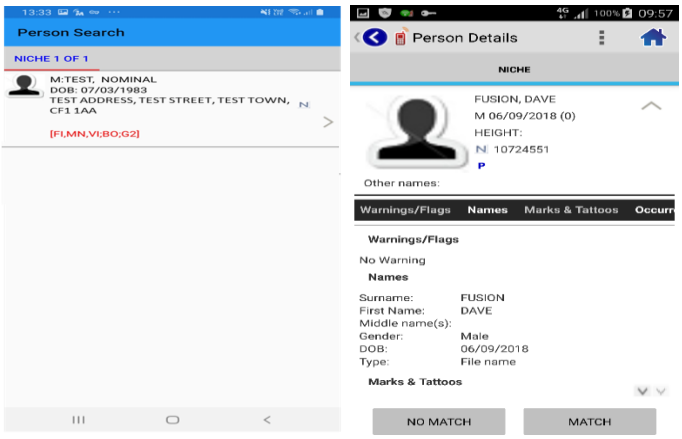
Searching within Candidate Images

7.16 If the Operator considers a Candidate Image to be a Possible Match, it is possible to search for further details by tapping on the Candidate Image. This will then generate a search screen allowing the user to determine the systems to be searched. The systems to be searched will be determined by the Operator's policing purpose. *(Below left)*

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



7.18 OIFR will then present the standard iPatrol search function, and will allow the Operator to navigate through Niche records in the usual way. *(Below)*

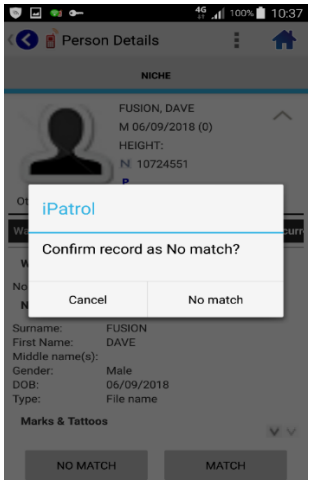


Auditability

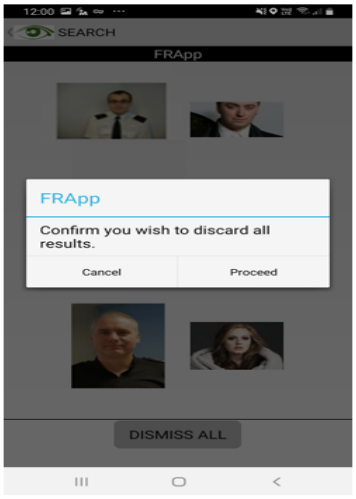
7.19 To ensure that use of OIFR can be properly audited and provide appropriate transparency and oversight, a mandatory audit requirement is included.

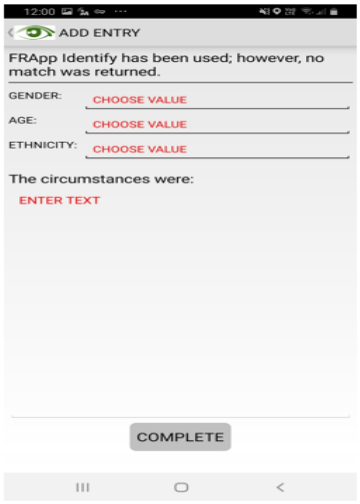
7.20 This takes the form of two buttons ‘NO MATCH’ and ‘MATCH’ which feature at the bottom of the Person Details screen. Selection of one of these buttons is mandatory to record the outcome of any search performed as a result of OIFR.

7.21 If the Operator determines as a result of searching the details of the Candidate Image that the Subject has not been successfully identified, NO MATCH must be selected. This will prompt the Operator to confirm. *(Below)* This will return the Operator to the original Candidate Images however with the previously chosen Candidate Image now greyed out.



7.22 If the Operator determines that none of the Candidate Images matches the Subject they should select 'DISMISS ALL'. *(Below left)* The user is then asked to confirm that they wish to proceed. This will present the Operator with a mandatory Audit screen to record the gender, age and ethnicity of the Subject along with any freetext. *(Below right)*

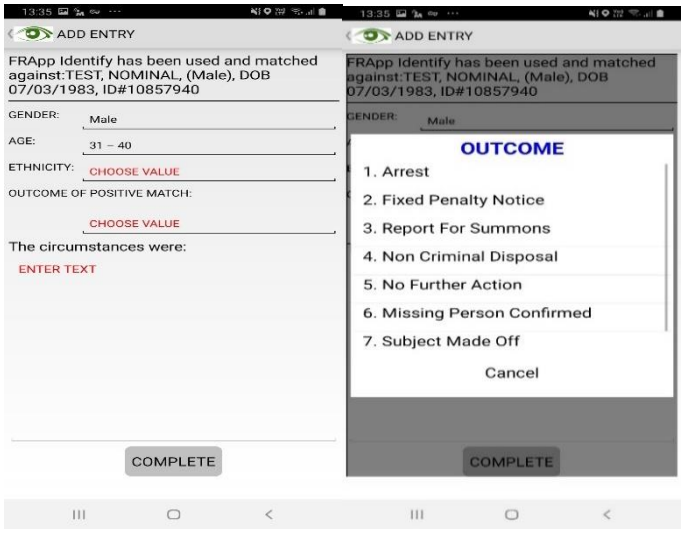




7.23 On completing the mandatory fields and pressing 'COMPLETE' at the bottom on the screen, the use of OIFR is now concluded.

7.24 If the 'MATCH' option discussed above has been selected, again there is a confirmation required from the Operator which if agreed then presents a mandatory returns form. 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 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.



Automatic Auditability – ePNB Ingestion

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

7.27 **A. OIFR Identify Search**

This entry automatically inserts into the ePNB of the Operator as soon as the search button is pressed.

Prior to the search button being pressed, no identifying information is provided for any Candidate Images.

This entry will automatically obtain a date and time stamp, GPS generated or manually recorded location and will further list the NICHE ID numbers of the individuals returned as part of the search.

The Operator has no means to edit or modify this entry

7.28 **B. OIFR Identify Record Viewed**

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

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

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

7.29 **C. OIFR Identify Match**

This entry is created if the "No Match" option is chosen. The ePNB log will record the circumstances and monitoring information of the Subject.

The content shown 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.

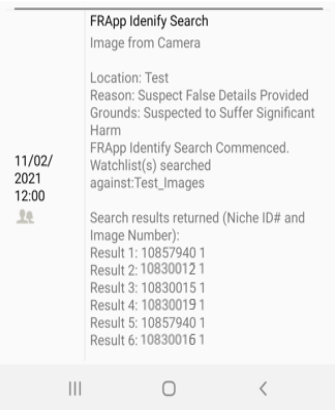
7.30 **D. OIFR Identify No Match**

This entry is created if the "Match" option is chosen. As above this entry reflects Operator input.

The content shown from a pre-defined drop-down menu.

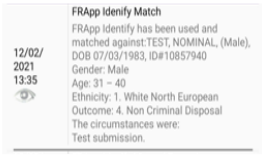
A free text field, in which the Operator is to record any other useful information to include any concerns raised during OIFR use

FRApp Identify Search EPNB Entry

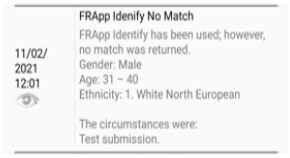


FRApp Identify Viewed Record EPNB Entry

FRApp Identify Match EPNB Entry



FRApp Identify No Match EPNB Entry



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

8 Image Reference Database(s)

8.1 OIFR will utilise SWP/GWP custody images and SWP 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 for the force area. It also includes live missing persons (deemed increased risk) for the SWP area.

8.3 The Image Reference Databases are a direct duplication of the images that are currently legitimately stored in Niche RMS, (SWP 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 where applicable officer safety (OST) training 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 the OIFR pilot. The SRO will liaise as necessary with NPCC ranked officers and the SWP Police and Crime Commissioner.

b) The Divisional Services Division Chief Superintendent is Chair of the Facial Recognition Technology and Biometric Board and is responsible for effective governance and accountability for the OIFR pilot.

c) The Digital Services Division FRT Project lead has tactical command of the OIFR pilot and is responsible for tactical implementation. They are also responsible for ensuring that the use of OIFR and their tactical implementation remains lawful, necessary, and proportionate throughout the duration of the OIFR pilot, having particular regard to the effectiveness of the safeguards in place whilst OIFR is being used.

Operator

11.2 The Operator is the officer operating OIFR, who is responsible for establishing the legal basis for using OIFR and considering Candidate Images for Possible Matches.

11.3 Operators receive detailed training prior to using OIFR operationally.

11.4 Operators must have an understanding of OIFR and the FRT System, how it performs, and what effect Subject, System, and Environmental Factors might have.

11.5 Operators may be deployed in uniform or plain clothes although the use of OIFR is to be in an overt manner.

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 has 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 officers 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 or detain. 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 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, any action taken, and have a lawful basis for doing so.

11.11 Where members of the public choose to exercise their right to avoid 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 Images 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.