SOUTH WALES POLICE / GWENT POLICE
POLICY DOCUMENT FOR THE OVERT USE OF OPERATOR INITIATED FACIAL RECOGNITION (OIFR)

Protective marking:	Official
Publication scheme Y/N:	No
Title:	Policy document for the overt use of Operator Initiated Facial Recognition (OIFR)
Version:	Version 1.1
Summary:	Guidance for South Wales Police / Gwent Police use of the OIFR 2024 pilot
Department:	Digital Services Division
Review date:	14/12/2025

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	01/06/2021	Project Lead	Ch. Insp Scott Lloyd	Initial Draft
0.2	21/09/2021	Project Lead	Ch. Insp Scott Lloyd	National terminology
0.3	03/11/2021	FRT Board	Governance Review	No Amendments
0.4	25/01/2022	DSD Head	Ch Supt Simon Belcher	Pilot Sign off. No Amendments
1.0	19/06/2024	Project Lead	Inspector Ben Gwyer	Update to include NPL findings
1.1	14/12/2024	Project Lead	Inspector Ben Gwyer	Final scrutiny amendments

Table of Contents

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

1 Introduction, Aim and Scope

Introduction

1.1 Operator Initiated Facial Recognition (OIFR) helps South Wales Police (SWP) and Gwent Police (GWP) identify people who are wanted for criminal offences and helps protect the most vulnerable in our society. More detail about how OIFR works and how SWP/GWP uses it can be found in section 3 (OIFR Overview).

1.2 This OIFR Policy Document provides SWP/GWP personnel with advice on the overt use of OIFR in a legally complaint and ethical manner to enable SWP/GWP to achieve legitimate policing aims.

1.3 This guidance specifically addresses a number of areas of concern highlighted on a local and national level. SWP/GWP is also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics Commissioner, and the Surveillance Camera Commissioner and is keen to support the development of national guidance and/or a code of practice relating to OIFR and its use by UK Law Enforcement Agencies (LEA).

1.4 SWP and GWP intend to conduct a force-wide pilot of OIFR to determine its effectivity and benefits to Policing. The Pilot will last 12 months, will remain under review to ensure that the continued deployment is meeting lawful policing objectives.

Aim & Scope

1.5 This guidance aims to: -

a) provide SWP/GWP personnel and members of the public with information about SWP/GWP's strategic, operational and technology objectives for the overt use of OIFR, such that it enables SWP/GWP to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives); and

b) provide SWP/GWP personnel with guidance on the use of OIFR by SWP/GWP in both public and private spaces to meet SWP/GWP's objectives for OIFR; and

c) establish the governance structure for the use of OIFR, ensuring that SWP/GWP use is appropriately governed and legally compliant; and

d) provide an overview of OIFR and advise on practical issues such as technology use (OIFR Device) in order to obtain the best performance from OIFR.

Not in Scope

1.6 There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR). RFR is also often referred to as 'post-event', which relates to non-real time searching of images against a database. Also, Live Facial Recognition (LFR) is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist(s) in order to locate persons of interest by generating an alert when a possible match is found.

1.7 In summary, this guidance does not extend to:-

a) manually instigated facial recognition for retrospective searching of video / still images; or

b) live facial recognition deployment utilising CCTV cameras; or

c) the legal framework that is applicable to SWP/GWP's use of OIFR – this is separately detailed within SWP/GWP's OIFR Legal Mandate Document.

Additional Documents

1.8 A number of documents are available to supplement this guidance and these include but are not limited to, the:-

a) SWP/GWP OIFR Standard Operating Procedure (SOP)

b) SWP/GWP OIFR Data Protection Impact Assessment (DPIA)

c) SWP/GWP OIFR Legal Mandate

d) SWP/GWP OIFR Appropriate Policy Documents

e) SWP/GWP OIFR Equality Impact Assessment

f) SWP/GWP OIFR Training Documents and User Guides.

2 Terminology

2.1 Within SWP/GWP and throughout SWP/GWP OIFR Documents, the following terms and definitions apply in relation to OIFR:-

Biometric Template	A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm and new templates will need to be generated from the original images if the Facial Recognition Technology (FRT) algorithm is changed.
Candidate Image	Image of a person in the Image Reference Database.
Environmental Factors	They are external elements that affect OIFR performance such as dim lighting, glare, rain, mist etc.
FRT System	The technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database generating probable matches. This is based on digital images (still or from live camera feeds)
Image Reference Database	A set of lawfully held known Candidate Images against which a Probe image is searched.
Match	A match occurs when the Operator, on viewing the Possible Matches, forms the belief that the Subject is identifiable as the same person shown in the Candidate Image.
No Match	The Operator determines as a result of viewing the Candidate Images and/or Possible Matches that the individual has not been successfully identified.
No Results Returned	A message returned to the Operator as no image has exceeded the Threshold Setting of 0.66 resulting in no Candidate Images being shown to the Operator
OIFR	Operator Initiated Facial Recognition (OIFR) is a mobile phone use of FRT technology, which compares a photograph of a person's face taken on a mobile phone to the predetermined Image Reference Database to assist an officer to identify a subject for a Policing purpose.
OIFR Device	Police issued mobile phone device from which the OIFR search is undertaken and to which any possible matches exceeding the Threshold Setting are returned.

Operator	The Police Officer/ Police Staff trained to utilise OIFR, who is responsible for establishing the legal basis for using OIFR and considering Candidate Images for Possible Matches. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of OIFR.
Person(s) of Interest	This term comprises persons on an Image Reference Database.
Possible Match	Operator considers a Candidate Image may be the same person as in the Probe Image resulting in police indices being further searched.
Probe Image	The facial image or footage submitted for a facial search against the SWP / GWP Image Reference Database.
Similarity Score	This is a numerical value indicating the extent of similarity between the Probe and Candidate Image, with a higher score indicating greater points of similarity.
Senior Responsible Officer (SRO)	Has strategic command for the use of OIFR. The SRO will liaise as necessary with NPCC ranked officers and the SWP/GWP Police and Crime Commissioner.
Subject	The individual whose image is obtained by the Operator for comparison via OIFR.
Subject Factor	A factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.
SWP/GWP OIFR Documents	SWP/GWP OIFR Documents that regulate SWP/GWP use of OIFR
System Factor	A factor relating to the FRT System such as the algorithm.
Threshold setting	The configurable point at which two images being compared will result in a match being returned. The threshold needs to be set with care to maximise the probability of returning high scoring non-matched subjects.

3 OIFR Overview

OIFR in a law enforcement context

3.1 OIFR helps SWP/GWP identify people who are wanted for criminal offences and helps protect the most vulnerable in our society.

3.2 OIFR also helps us identify those posing a risk of harm to themselves or others. Images obtained using OIFR are searched against an Image Reference Database of people who are wanted, or based on intelligence are suspected of posing an immediate threat to life or immediate risk of serious harm to themselves or others,

3.3 The FRT System works by analysing key facial features to generate a mathematical representation of them (Biometric Template). This representation is then compared against the Biometric Templates of known faces (Candidate Images) in an Image Reference Database in order to identify Possible Matches for Persons of Interest. When the facial features from two images are compared the FRT System generates a Similarity Score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. The top six similar Candidate Images that score above the Threshold Setting are returned to the Operator. If less than six images exceed the Threshold Setting, only the Candidate Images that have scored above the Threshold Setting will be returned for the review of the Operator. In this way, OIFR works to assist SWP/GWP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

OIFR and South Wales Police (SWP)/Gwent Police (GWP)

3.4 OIFR is a valuable policing tool that helps SWP/GWP to keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

3.5 The following are illustrative examples where OIFR may assist SWP/GWP with its policing purposes:-

a) Supporting the identification and arrest of people wanted for criminal offences;

b) 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, sex offenders etc.);

c) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed.

d) Supporting the identification of deceased persons, to assist the coroner.

3.6 Whilst appropriate use of OIFR delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of OIFR involves biometric processing. SWP/GWP is conscious that the use of OIFR will be the subject of much debate. Areas that are likely to be subject of particular debate and scrutiny relate to any intrusion into civil liberties, the potential for the imbalance of use towards persons that may not be able to understand officers request for personal information (i.e. Subjects with learning difficulties, children or foreign nationals) and the possibility for automated decision making as a result of the use of OIFR.

3.7 It is therefore incumbent on SWP/GWP to ensure that OIFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of OIFR.

3.8 In seeking to address other potential concerns, SWP/GWP has undertaken independent academic research in conjunction with Metropolitan Police Service (MPS) and National Physical Laboratory (NPL) for FRT, and has proactively engaged with civil liberty interest groups and South Wales and Gwent Police and Crime Commissioner's Office.

3.9 SWP/GWP has listened carefully to many parties with an interest in the use of OIFR and has carefully considered what safeguards are necessary to support the use of

OIFR. When and where OIFR can be used has been carefully designed with clear documented objectives. The Senior Responsible Officer (SRO) must ensure that the strategic use clearly articulates legality, necessity and proportionality.

3.10 The SRO must also be satisfied that Operators using OIFR are appropriately trained, briefed, and accountable.

3.11 The SRO must also consider how use of OIFR may impact on communities as a whole, and how the rights of everyone whose image is likely to be captured by use of OIFR have been considered, and what safeguards are in place to protect them.

3.12 SWP/GWP is not only concerned with developing and implementing policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as OIFR, are monitored for impact. SWP/GWP will implement a robust governance process to review the effectiveness and impact of OIFR during the 12 month pilot. SWP/GWP will focus on delivering transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from South Wales and Gwent communities as part of an ongoing process.

3.13 This guidance document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

4 Strategic Intention, Objectives and Use Case

4.1 OIFR use must comply with the following strategic intentions and operational objectives.

Strategic Intentions

4.2 SWP/GWP will:-

a) use overt OIFR in a responsible way to identify offenders and vulnerable persons in accordance with SWP/GWP's common law policing powers. This includes targeting those wanted for offences, and

b) comply with the common law and statutory safeguards in delivering its policing operational duties, and relies on the common law to discharge a number of its duties. OIFR can assist with SWP/GWP's duties to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security. This includes targeting those wanted for offences. It also includes using OIFR to protect the public, reduce crime and help safeguard vulnerable persons.

c) strengthen and develop OIFR capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep South Wales and Gwent safe.

d) build public trust and confidence in the development, management and use of OIFR by taking account of privacy concerns and maximising transparency; and

e) maintain good governance through a command structure that incorporates strategic, operational and technical leads for the use of OIFR, with clear decision making and accountability; and

f) ensure that the use of OIFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Surveillance Camera Commissioner, the Information Commissioner and SWP/GWP OIFR Documents; and

g) transparently identify, manage and mitigate reputational and organisational risk to SWP/GWP; and

h) be recognised as a responsible, progressive and ethical organisation

Operational Objectives

4.3 SWP/GWP will:-

a) use OIFR to enable SWP/GWP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities such as violent crime. OIFR will increase intelligence-led enforcement opportunities including those relating to knife and gun crime, child sexual abuse, terrorism, and helping to safeguard vulnerable persons. It will also help identify those wanted by the courts or in breach of their bail conditions; and

b) adopt a robust and proportionate approach in engaging and pursuing individuals identified on an Image Reference Database, using human decision-making. Operator oversight is active and involved, with the Operator retaining full control and making the decision as to whether a match is made, and following a match confirmed by the Operator, what action is most appropriate to dispose of the engagement; and

c) engage with and provide reassurance to communities, listening and responding to concerns; and

d) continually identify and review risks relevant to OIFR, mitigate those risks, and maintain a response plan should mitigation fail; and

e) identify best practice and lessons learnt from the use of OIFR in the operational environment to improve outcomes and to maintain public confidence.

Technological Objectives

4.4 SWP/GWP will:-

a) ensure all OIFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and

b) provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other offences; and

c) look to technological improvements whilst keeping the SWP/GWP OIFR SOPS under review. Where appropriate we will trial alternative providers of

facial recognition software and hardware in parallel with our current provision. This helps to ensure that the best possible service is sought, and we are able to proactively develop improved working methodologies and accuracy. The outcomes of any parallel trial will be captured with the same key performance metrics that are gathered when deploying OIFR to ensure the findings are suitable for direct comparison and analysis. All previously detailed retention periods will remain unaffected. Personal information that is processed in this manner will not be shared with any third-party individual.

Use Case

4.5 This guidance relates to the use of OIFR in an overt capacity to help SWP/GWP protect the public. SWP/GWP will keep the use of OIFR under review to ensure OIFR continues to be used as an effective crime fighting tool.

4.6 OIFR helps SWP/GWP use its resources more efficiently. SWP/GWP considers that OIFR is better than humans at recognising persons from a large dataset (generally thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to SWP/GWP to include any potential risks posed by the Subject.

4.7 The way in which OIFR is utilised by SWP/ GWP Operators will be kept under strict review, OIFR will be used where it has the greatest potential to assist SWP/GWP in discharging its operational duties.

4.8 Given that use of OIFR requires an Operator to review all Candidate Images for a decision as to whether any further action is required, SWP/GWP will always use OIFR in a way that is operationally effective and allows SWP/GWP to act on any Candidate Images as they are generated. OIFR will not be used indiscriminately.

5 Overview of OIFR Use

End-to-End Process

5.1 The end-to-end process of the use of OIFR can be summarised as follows:-

a) The Officer will interact with the subject for a lawful Policing purpose. The Officer should make all reasonable attempts to ascertain the identification of the individual via traditional and less intrusive means. During this engagement, the Officer may form reasonable grounds to suspect that at least one of the identified reasons and one of the identified grounds for the use of OIFR exist

b) Where the Operator has formed the opinion that OIFR is necessary to identify the individual, they will activate their Body Worn Video (BWV) to capture the interaction. If for any reason, BWV is not being used, the Operator must record the reason why.

c) The Operator will record whether the OIFR use is in a private place or a public place, the Officer defined gender, age and ethnicity of the subject.

d) The Operator will identify the Image Reference Database the comparison will be conducted against. The selection of Image Reference Database should be proportionate and considered against the circumstances justifying OIFR use

e) The Operator will record the circumstances that justify the necessity to use OIFR and the location of OIFR use. This should include what less intrusive enquiries have been undertaken to identify the Subject prior to OIFR being used.

f) The Operator will capture the Probe Image of the subject via the OIFR app. The capture will only be conducted via the app as following the OIFR comparison, the Probe Image will not be retained in any form on the device or otherwise. The Operator should consider the location before capturing the Probe Image to ensure that as far as practicable, collateral intrusion does not occur.

g) The Operator will be offered the opportunity to review the Probe Image captured. If the Probe Image is not of sufficient quality, the Operator will be able to retake the image. If the Operator decides to retake the image, the original image captured will be automatically deleted and will no longer be retrievable. If the image is good enough quality, the Operator should use the in app cropping tool to crop the image to prevent any collateral intrusion of any person other than the subject in the Probe Image

h) The Officer will then submit the Probe Image for comparison against the selected Image Reference database(s). The OIFR app will return matches that score above the Threshold Setting or will return no results if no Candidate Images Similarity Score exceeds the Threshold Setting.

i) The Operator will review any potential matches returned and will make the determination as to whether the OIFR app has returned a correct match. The Operator will record the match as ‘MATCH’ or ‘NO MATCH’ on the OIFR app.

j) If no match is made, the Operator will provide a short rationale

k) If a match is made, the Operator will record the outcome of the interaction with the subject i.e arrest, stop search

l) If the Operator decides that the use of OIFR is no longer justified, they will discard the search. If the search is discarded, the Operator will record the reason for discarding the search.

5. 2 SWP/GWP OIFR SOP provides a greater level of detail about where and when OIFR may be used by SWP/GWP.

Key Points

a) OIFR uses images of Subjects (Probe Image) obtained by the Operator. The Probe Image must be taken then and there and cannot be uploaded from a camera gallery.

b) The cameras on the OIFR Devices have been selected for use as the quality of images they produce are vital to ensure a Probe Image of sufficient quality is achieved.

c) The quality and resolution of images (both those in the Image Reference Database and those from the OIFR Device camera) are of vital importance and must be carefully considered.

d) The inclusion of persons on an Image Reference Database needs to be justified based on the principles of necessity and proportionality

e) It is important to balance the objectives of the use of OIFR with the size of the Image Reference Database and the available resource to respond to Possible Matches.

f) 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.

g) Wherever possible OIFR must 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.

h) OIFR will form the intelligence and information stages of the National Decision Making Model

i) OIFR will be used to assist confirm the Identity of a Subject and or provide the potential risks posed by the Subject. OIFR will be used to support and not replace other policing tactics; to include powers of search and or a power of arrest.

6 Governance, Oversight and Impact Assessments

6.1 SWP/GWP OIFR Documents address the stipulations detailed above. 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.

Pre – Operational Use

6.2 Prior to any use of OIFR, the Operator must have undertaken the relevant OIFR training provided by Digital Services Division. Access to the OIFR system will not be provided to Operators until this training has been completed. This access is only available via a SWP/ GWP Issued mobile phone device and cannot be transferred to other devices.

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

6.4 The outcomes of any OIFR searches, even those discarded before completion, will be 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.

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

Key documents available to the public	**Information included**
SWP/GWP OIFR Legal Mandate	• The lawful basis for processing data in relation to OIFR. Including in relation to: o Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Protection of Freedoms Act 2012 o Data Protection Act 2018 • Freedom of Information Act 2000
SWP/GWP OIFR Policy Document	• An outline, strategic intent and objectives for the use of OIFR and how personal data will be used by the FRT System • Data retention periods applicable to OIFR
SWP/GWP OIFR, SOP Processes	• Outlines measures relevant to considering when OIFR can be used by SWP/GWP. o Reference Image Database considerations including the basis on which images may be added to an Image Reference Database.
SWP/GWP OIFR Data Protection Impact Assessment (DPIA)	• Describes the nature, scope, context and purposes of the processing. • Assesses necessity, proportionality and compliance measures.

	• Identifies and assesses risk to individuals. Identifies any additional measures to mitigate those risks.
SWP/GWP OIFR Appropriate Policy Documents	• Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the Data Protection Act (DPA) 2018. • Explains how the processing of special category data under Part 2 DPA 2018 and Article 9 General Data Protection Regulation • Explains how SWP/GWP complies with the Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of personal data.
SWP/GWP FRT Equality Impact Assessment	• Promotes all aspects of equality. • Ensures compliance with the law, taking into account of equality and human rights.

Operational Use

6.6 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.

6.7 At the outset of an OIFR search, the OIFR app will create an entry in the ePNB of the Operator. This will record the date of the search, the time, whether the search was conducted in a public or a private place, 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.

6.8 The Operator will obtain a suitable Probe Image 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.

6.9 The OIFR search will be undertaken with body worn video being utilised to record the interaction

6.10 The OIFR app will return up to six Candidate Images that exceed the OIFR Threshold Setting for the Operator to consider. The Operator will review the images and make a determination if a match has been made. 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 for comparison and also then move into the Ipatrol app, PNC or warrants management system in order to review available information.

Post use

6.11 At the conclusion of the search, if a match has been made, the Operator will record the outcome of the interaction and search. This will be recorded in the ePNB of the Operator automatically by the OIFR app.

6.12 The Operator will be responsible for ensuring that BWV recordings of their interaction with the subject are properly categorised and retained

6.13 SWP/GWP must 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.

6.14 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.

6.15 The outcome of OIFR uses must be subject of ongoing evaluation, which in turn should feed into oversight and scrutiny processes.

Following consultation the following stipulations have been proposed and accepted by SWP/ GWP:-

a) The overall benefits to the public must be great enough to sufficiently compensate for the potential public distrust it may invoke;

b) It can be evidenced that the technology itself will not result in unacceptable gender, age or racial accuracy variance into policing operations;

c) The strategic use of OIFR must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific policing purpose;

d) Operators are trained to understand the risks associated with use of the software, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions;

e) SWP/GWP, will develop and maintain robust governance and oversight arrangements that balance the technological benefits of OIFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency, whilst taking into account guidance from relevant Commissioners and Regulators. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

Governance Framework

6.16 SWP/GWP OIFR documents address the stipulations detailed above. Governance and oversight of the use of the technology is realised by maintaining a 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 Programme Board which will review the performance outcomes of OIFR and tactical deployment of the technology.

b) The Division Commanders will have tactical command for the deployment of OIFR within their geographical areas of responsibility. It will be their responsibility to ensure effective governance of the technology and accountability of the Officers deploying OIFR in their geographical areas of responsibility. 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

6.17 SWP Ethics Committee are an independent source of advice. Their terms of reference include the provision of advice and independent oversight of SWP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework.

6.18 The SWP Police and Crime Commissioner and the Gwent Police and Crime Commissioner have a key role in the scrutiny and oversight of OIFR as part of the wider principal of holding the Chief Constable to account on behalf of the public.

6.19 Circumstances may arise that mean that there is a need to suspend an Operator's permission to utilise OIFR on the basis of training needs or otherwise. In this circumstance, the rationale should be formally documented and permission to use OIFR is to be suspended immediately. This permission should not be provided to the Operator again until any performance, training or misconduct matters to which OIFR use relates are concluded or if the suspension of OIFR use relates to performance/ training need, that the Operator has undergone training and the FRT Lead is satisfied that they have met the necessary requirements to be afforded permission to access the OIFR capability

6.20 The outcomes of use of OIFR must be subject of evaluation, which in turn should feed into the oversight and scrutiny processes.

6.21 ePNB - the MOPI retention of personal information (detailed within ePNB DPIA), not including the Probe Image.

7 Oversight Bodies and Regulatory Framework

7.1 Within SWP/GWP, the senior internal oversight body for OIFR is SWP FRT & Biometrics Programme Board, which in-turn answers to the SWP Gold Board. In addition, the South Wales Police and Gwent Police Crime Commissioner's Office also provide an external oversight and scrutiny perspective.

7.2 SWP/GWP OIFR Legal Mandate sets out the legal framework for SWP/GWP use of OIFR, whilst SWP/GWP OIFR Policy Document and SWP/GWP OIFR SOP support implementation.

7.3 Nationally, the `NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.

7.4 Further oversight opportunities may arise in relation to the `Joint National Biometric Strategic Board'. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the Information Commissioners Office, the Surveillance Camera Commissioner, the Biometric Commissioner and the National Policing Chief Scientific Adviser. More detail on these roles: -

a) Biometrics and Surveillance Camera Commissioner (BSCC); The role of the Biometrics and Surveillance Camera Commissioner is to:

- keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints.
- decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984)
- review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints
- provide reports to the Home Secretary about the carrying out of his functions
- encourage compliance with the Surveillance Camera Code of Practice
- review how the code is working
- provide advice to ministers on whether or not the code needs amending

The commissioner is independent of government. The commissioner has no enforcement or inspection powers regarding surveillance cameras and works with relevant authorities to make them aware of their duty to have regard to the code.

See About us - Biometrics and Surveillance Camera Commissioner - GOV.UK (www.gov.uk)

b) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Privacy Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

See www.gov.uk/government/organisations/information-commissioners-office;

c) National Police Chief Scientific Adviser (NPCSA); The role of the Chief Science Advisor is provide Police Chief Officers with advice on all aspects of policy on science and technology.

See www.gov.uk/government/groups/chief-scientific-advisers

8 Public Engagement

8.1 Public engagement must be supported by the use of online resources available to the public, which should be underpinned by a press and media strategy relating to the use of OIFR. During OIFR use and where practicable information, including details of the Privacy Notice, should be distributed and feedback via email should be sought.

8.2 Operational briefings delivered to officers and stakeholders prior to OIFR use should promote openness with the public and transparency about the use of OIFR. Officers should be encouraged to engage with the public to increase awareness of how OIFR helps keep the public safe and how it helps bring offenders to justice. It is also helpful for officers to be in possession of notices that can be handed out to the public. Such notices should deliver important key messages aimed at promoting trust and confidence through improved understanding.

8.3 Key stakeholders, including the Police and Crime Commissioner's Office, may be invited to observe the planning and use of OIFR.

In Advance of OIFR use

8.4 In advance of OIFR SWP/ GWP will ensure that: -

a) The intention to provide Operators with OIFR capability is notified to the public using SWP/GWP website and other appropriate communication channels (including social media). The notification will advise that OIFR may be used by Operators in the course of lawful policing duties and will not be specific for each opportunity to where OIFR will be used; and

b) literature is prepared for Subjects (to include information outlined within a privacy notice); and

c) Operators are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a Constable in uniform to compel a person to remove anything that conceals their identity; and

d) external engagement is considered in discussion with SWP/GWP FRT team. It may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies.

During OIFR Use

8.5 When OIFR is being used, SWP/ GWP will ensure that: -

a) notices with a brief explanation and reference to SWP/GWP website are available to the public on request; and

b) information is provided to Subjects in accordance with the policy referred to above.

After Use

8.6 After OIFR use ensure that: -

a) information about OIFR use, including location, time, date, engagements, outcome, and any other information considered helpful and suitable for disclosure, is captured in the officer's ePNB; and

b) external engagement is considered in discussion with SWP/GWP FRT team. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the FRT team must be consulted prior to this kind of activity.

9 Image Reference Database Considerations

Image Quality

9.1 The performance of the FRT System is heavily dependent on the quality of the images in the Image Reference Databases. The best images are those that follow a custody or passport style image that conforms to the NPIA 'Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'. Further detail is included within the embedded PDF:

NPIA Standard Still Digital Images.pdf

9.2 Where multiple images of a Subject are available, consideration should be given to including these in the Image Reference Databases where it is advised that they will improve the likelihood of identifying those of interest to SWP/GWP.

Accessible Image Reference Database(s)

9.3 SWP/GWP Legal Mandate provides commentary on the legal considerations relevant to compiling an Image Reference Database in a lawful way. This means that we ensure

we hold Candidate Images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes.

9.4 Key points include ensuring the Image Reference Database is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Image Reference Database. SWP/GWP OIFR SOP provides practical guidance on how to follow SWP/GWP OIFR Documents, including SWP/GWP OIFR Legal Mandate.

9.5 OIFR will utilise the SWP and GWP custody images and SWP/GWP images of missing persons. Candidate Images and their related Biometric Template reside on the FRT System and not the officer's mobile device.

Governing the Image Reference Database(s)

9.6 The FRT Systems used to generate Image Reference Databases are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

9.7 SWP/GWP OIFR Documents provide measures to ensure that the Image Reference Databases are lawfully compiled, current, is not retained beyond its purpose, and is only used for its FRT purpose.

Addressing Disproportionality

9.8 SWP/GWP will retain a breakdown of officer defined race, gender and age of Subjects as well as the circumstances for use.

9.9 The use of OIFR is driven by SWP/GWP policing priorities, information and intelligence-led assessments, both of which determine locality and the policing purpose.

9.10 SWP/GWP recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. Detailed equitability testing has taken place prior to the provision of OIFR to operational staff, see FRT EIA for further details.

9.11 As part of SWP/GWP's ongoing obligation with regards the Equality Act 2010, SWP has undertaken equitability testing of OIFR and the FRT System by the National Physical Laboratory. The necessity and frequency are determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms. The findings of this study can be accessed at:

frt-equitability-study_mar2023.pdf (science.police.uk)

9.14 When equitability tests are conducted, no biometric data belonging to members of the public is retained for law enforcement purposes. Images and recordings are only retained for the purpose of the future testing with the prior consent of those involved in the testing.

9.15 SWP/GWP has a number of measures to guard against a System Factor (system bias) affecting the generation of returned Candidate Images. These measures include that:

a) those involved in the use of OIFR monitor returned Candidate Images, Subject Factors, System Factors and Probe Images throughout the use of OIFR. Should concerns arise that OIFR is not performing correctly, the SRO will halt the use of OIFR where necessary; and

b) for the purpose of facilitating post-OIFR reviews, the elements of OIFR use are recorded in the officer's ePNB. It provides further opportunity to consider the Subject, System and Environmental Factors, returned Candidate Images, and the effectiveness of the safeguards in place for OIFR, including the reviews undertaken by the attendees of the FRT and Biometrics Board and SRO; and

c) in the event post-OIFR use reviews identify an area of concern, SWP/GWP may undertake further demographic accuracy variance testing where this appears necessary.

10 Design Guidelines for OIFR

10.1 A new international standard (ISO IEC 30137-1: `Use of biometrics with video surveillance systems, Part 1: System design and specification)' was published in May 2019. See www.iso.org/standard/64935.html.

10.2 SWP/GWP OIFR processes and associated guidance has been developed so as to provide for a reliable means of identifying individuals using OIFR with high-definition mobile phone cameras (8MP and above). For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the Operator, and associated policing resources on the ground.

10.4 A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this guidance.
Directly relevant components include:

a) the OIFR Device camera, and its use in proximity and angle to the Subject's face; and

b) the environment in which the cameras operate; and

c) Image Reference Databases and associated meta data; and

d) the FRT System that detects face in the Probe Image, converts the facial images into Biometric Templates, compares these against the Image Reference Database(s) and provides information on the results of the comparison to the Operator; and

e) the Operator who assesses the Candidate Images and determines the appropriate course of action; and

f) having sufficient officer resource to support the use of OIFR.

11 OIFR Device Camera and Camera Use

11.1 The OIFR Device camera must be selected so that the image resolution, field-of-view and low-level light performance can provide images of sufficient quality for use in the FRT System. Currently FRT Systems typically require a facial image with between 20 and 100 pixels between the centres of the Subject's eyes (Inter-Eye Distance or IED). The FR vendor should advise on specific requirements for their system.

11.2 Unless the environment is well controlled, cameras must be capable of operating at Wide Dynamic Range in order to generate high quality images under a variety of lighting conditions.

11.3 Cameras should ideally be positioned to capture faces as close as possible to the 'face-on' condition, similar to a passport image.

11.4 Ideally the environment should be managed to ensure the Subject's face is evenly illuminated. Highly directional lighting, for example strong sunlight, should be avoided, which may require consideration of how the lighting will change throughout the day.

11.5 In low light conditions the automatic setting for the mobile phone camera will allow the face to be illuminated using the phones led flashlight.

11.6 Ideally Subjects should be 1.5 to 2 metres from the mobile phone camera when an image is captured (this will also allow a reactionary gap for the Operator).

12 Key Performance Metrics

12.1 This section covers some of the key performance metrics that should be gathered when using OIFR. It outlines the minimum requirements and so additional metric, or indicators may well be relevant and suitable for collation and analysis.

12.2 The Operator's ePNB will record details of OIFR use to include whether a Match or No match has been made and the related outcome.

12.3 The Similarity Score of all returned Candidate Images will be recorded for analysis and will not be available to the Operator.

12.4 The Threshold Setting for all OIFR searches is set to 0.66 following the advice of the National Physical Laboratory Equitability Study. This Threshold Setting is not configurable by the Operator and only the Candidate Images where the Similarity Score exceeds the Threshold Setting will be returned for review by the Operator. The maximum number of images that could be presented to the Operator is up to 6.

12.5 The Similarity Score for all returned Candidate Images will be recorded in the Operator's ePNB.

13 OIFR Guidance Summary

13.1 This guidance relates to the operational use of OIFR, and the governance and oversight regimes necessary to support its use.

13.2 Officers and staff must adhere to the guidance as this will help ensure that SWP/GWP use of OIFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.

13.3 This guidance will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are not covered within this guidance, it is essential these decisions are fully documented, together with detailed rationale, and that the relevant decision-making features within debrief and evaluation processes.