METROPOLITAN POLICE

More Trust | Less Crime | High Standards

MPS OIFR POLICY DOCUMENT

Direction for the MPS use of Operator Initiated Facial Recognition

Terms & Definitions: Capitalised terms used within this policy shall have the meaning given to them in Annex A of this document unless otherwise defined.

Table of Contents

1 Policy overview 3
2 Permitted OIFR use cases 3
3 How it works 5
4 Acquisition of Probe Images 6
5 Permitted Probe Subjects 7
6 Permitted Image Reference Libraries 8
7 Proportionality 8
8 Use of the OIFR System 13
9 Audit and reporting 16
10 Governance and oversight 16
11 Data management 17
12 Transparency 19
Annex A: Terminology 21
Annex B: Types of FR 23
Annex C: Imagery 24
Annex D: Imagery and Protected Characteristics 27
Annex E: Proof of Concept 30

Protective marking:	Official
Publication scheme Y/N:	No
Title:	OPERATOR INITIATED FACIAL RECOGNITION: POLICY
Version:	1.0
Summary:	Direction for the MPS use of Operator Initiated Facial Recognition
Branch/ OCU:	MPS FR
Review date:	1 November 2027

1 Policy overview

1.1 Officer Initiated Facial Recognition ("OIFR") is an overt[1] digital policing capability with which the MPS compares a Probe Image depicting a Permitted Probe Subject, obtained for the purposes of a search, against images in Permitted Image Reference Libraries in order to assist an OIFR User in determining whether there is a Viable Match. Any Potential Match generated by the OIFR System[2] does not, of itself, establish identity and must be subject to adjudication by an OIFR User, who will determine whether the Potential Match constitutes a Viable Match.

1.2 The Policy sets out the principles and procedures which govern the MPS's approach to OIFR use, as well as explaining at a practical level how OIFR operates. The Policy also adopts a set of defined terms to ensure precision and consistency in the description of OIFR and its use by the MPS.

1.3 Pursuant to this policy, the MPS may only use OIFR:

a) in a permitted 'Use Case' (as defined in Section 2 below);

b) where the Probe Image has been acquired pursuant to Section 4 of this Policy and the subject depicted in the Probe Image captured and submitted to the OIFR System is a Permitted Probe Subject (as set out in Section 5 below);

c) against Permitted Image Reference Libraries (as set out in Section 6 below);

d) in compliance with the rules on Images (as set out in Annex C below);

e) in compliance with the rules on Protected Characteristics (as set out in Annex D below);

f) where its use is proportionate in all the circumstances (in accordance with the guidance in Section 7 below); and

g) subject to the requirements as to transparency set out in Section 12 below.

1.4 Sections 2 - 12 of this policy contain further guidance on the lawful use of OIFR by the MPS.

2 Permitted OIFR use cases

2.1 Pursuant to this policy, the MPS may only use OIFR in the context of the following distinct use-cases, which are set out in more detail below:

a) **Use Case A:** To support the identification of a subject for a law enforcement purpose[3].

b) **Use Case B:** To ascertain if an arrested or otherwise detained person poses a risk to themselves or others.

[1] This means OIFR must not be used in circumstances amounting to intrusive surveillance or directed surveillance.
[2] Other Facial Recognition systems are beyond the scope of this Policy.
[3] As defined by section 31 of the Data Protection Act 2018.

2.2 **<u>USE CASE A</u>: TO SUPPORT THE IDENTIFICATION OF A SUBJECT FOR A LAW ENFORCEMENT PURPOSE**

2.3 Where Use Case B does not apply, OIFR may be used to support the identification of a subject where:

a) Either:

i. the identity of a subject depicted in a Probe Image is unknown; or

ii. there are reasonable grounds for doubting that the identity being considered against the subject is the true identity of that subject; and

b) identification of the subject is necessary for a law enforcement purpose.

2.4 When using OIFR pursuant to Use Case A, the OIFR User must:

c) be lawfully present at the location from where the image is obtained;

d) obtain the image overtly and from a distance that would enable the OIFR User to engage with the subject;

e) be readily identifiable as a police officer, whether by being in uniform, displaying police-marked clothing or equipment, producing a warrant card, or by other appropriate means.

2.5 The transparency requirements applicable to Use Case A are set out in Section 12.

2.6 **<u>USE CASE B:</u> TO ASCERTAIN IF AN ARRESTED OR OTHERWISE DETAINED PERSON POSES A RISK TO THEMSELVES OR OTHERS**

2.7 OIFR will[4] be used in order to ascertain whether a person poses a risk to themselves or others where:

a) that person has been lawfully arrested or otherwise detained pursuant to a statutory power; and

b) there is a statutory power to obtain the detained person's photograph for a law enforcement purpose.

2.8 The purpose of Use Case B is to support the safe, lawful and effective management of an arrested or otherwise detained subject. Subjects can be safely managed only if officers are aware of any circumstances giving rise to a risk to the detained person or others, including (for example) any history of self-harm, attempted self-harm or suicide, and any history of violence towards police officers or otherwise. OIFR will assist by enabling identity-related information to be obtained at the earliest practicable stage following arrest or detention. In particular, the use of OIFR in Use Case B may uncover relevant information that would not be uncovered by a search of the name given by the subject on police databases, for example because such information is linked only to aliases or alternative identities of the subject, or is linked to

[4] See Annex E concerning the Proof of Concept.

images of a previously unidentified subject[5], or because the subject has given a false name. OIFR does not replace existing arrest and detention processes. Rather, it provides an earlier opportunity to obtain information capable of informing those processes and supports a more assured assessment of identity than reliance solely on biographical identifiers.

2.9 When using OIFR pursuant to Use Case B, the OIFR User must comply with any applicable Code of Practice relating to the taking or use of photographs.

2.10 The transparency requirements applicable to Use Case B are set out in Section 12.

3 How it works

3.1 The core technical operation of the MPS OIFR System in relation to a single Permitted Probe Subject using the OIFR system on a hand-held device can be summarised in nine stages as follows:

Stage	Action
1	**Permitted Image Reference Library Enrolment**
	A Permitted Image Reference Library is 'enrolled' into the OIFR System[6]. The OIFR software detects and analyses the facial features shown by the images in order to then express those features as a set of numerical values (i.e. a Biometric Template).
2	**Facial image acquisition**
	An approved OIFR User will initiate the process to capture an image depicting a Permitted Probe Subject into the OIFR System.
3	**Face selection**
	The OIFR User will consider if the face presented/manually selected is of the Permitted Probe Subject. The OIFR User will only proceed with the selected image for an OIFR Search for the purposes of a Permitted OIFR Use Case against the face of the Permitted Probe Subject. This stage operates as a data-protection-by-design safeguard to limit the processing of biometric data for the purpose of uniquely identifying a subject to cases where such processing is necessary and justified in accordance with this Policy.
4	**Face detection**
	The OIFR System pre-processes the Probe Image and detects the face(s) in the image. Where there are multiple faces in an image, or the OIFR System does not detect a single face, these results are presented to the OIFR System User.
5	**Feature extraction**
	From the face selected/confirmed by the OIFR User, the OIFR System produces a Biometric Template based around extracted key facial features.
6	**Face comparison**

[5] For example, the arrested subject may also feature within the Unsolved Crime Cache. Information obtained through OIFR may identify links to other offending of a different nature or seriousness, which may materially alter the assessment of threat, harm and risk and inform the management of the arrest or detention.

[6] The OIFR System will compare the probe image against the image reference library that is a subset of the MPS Custody images, this subset of images are based on custody image retention rules, as set out in Section 11.

	The OIFR software then compares the Biometric Template(s) of the Probe Image against the Image Reference Library.
7	**Matching**
	When the Biometric Template from the Permitted Probe Image is compared to the Permitted Image Reference Library, the OIFR System generates a similarity score against each image comparison. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. Results which exceed the threshold[7] (including the similarity score) will be presented to authorised OIFR Users as further described at paragraph 8.7 and 8.8 of this Policy.
8	**Adjudication**
	The rank one result will be returned to the OIFR User, this being the highest ranked image based on similarity score. The OIFR User, who is trained on the use of the OIFR system will assess the Potential Match and make a determination as to whether they consider this match to be viable, and if so, whether any further action is required.
9	**OIFR data destruction**
	The OIFR System will delete data in line with Section 11 of this Policy.

4 Acquisition of Probe Images

4.1 This policy does not confer any legal power on officers to photograph a subject. Nor does this policy confer any legal power to compel a person to cooperate in the taking of a Probe Image.

4.2 When OIFR is deployed under Use Case A, photographs will be taken in reliance on either (a) real and informed consent for its use in an OIFR search or (b) the common law power to take a photograph from a lawful vantage point without compulsion. Where practicable to do so without compromising operational objectives, consent should be sought before any common law power is used.[8] If consent is sought and withheld, this does not of itself prevent the taking of a photograph pursuant to a lawful common law power, provided the requirements of this Policy are otherwise met. The OIFR User:

a) Will capture images by using a MPS device approved for OIFR use; and

b) Must:

i. be lawfully present at the location where the image is obtained;

ii. obtain the image overtly. This means that the image must <u>not</u> be obtained in a manner that is calculated to ensure that the subject is unaware that they are being photographed; and

iii. be readily identifiable as a police officer, whether by being in uniform, displaying police-marked clothing or equipment, producing a warrant card, or by other means.

[7] Refer to the DPIA for detail as to the threshold configuration.

[8] Whether or not the subject consented should be recorded on body worn video (if possible, see paragraph 12.2(g)) and in writing as soon as practicable.

4.3 When OIFR is deployed under Use Case B, photographs will be taken in reliance on statutory powers to take a photograph of a detained person:

a) Section 64A of the Police and Criminal Evidence Act 1984;

b) Section 26(1) of the Counter Terrorism and Border Security Act 2019;[9]

c) Paragraph 2 to Schedule 8 of the Terrorism Act 2000

d) Paragraph 2 to Schedule 6 of the National Security Act 2024

e) Paragraph 18 to Schedule 2 of the Immigration Act 1971.[10]

4.4 Under Use Case B:

a) Images will be captured by using approved MPS imaging equipment, authorised for OIFR use including mobile devices or a camera in a policing facility where a subject is detained.
b) Images must be obtained in compliance with the applicable Code of Practice.

4.5 Under either Use Case, any photograph used as a Probe Image must:

a) have been lawfully obtained;
b) comply with the rules on Images (as set out in Annexes C and D below).

5 Permitted Probe Subjects

5.1 **Permitted Probe Subjects**

5.2 The circumstances in which a person may constitute a Permitted Probe Subject differ according to the applicable Use Case. The fact that a photograph may lawfully be obtained does not, of itself, permit its use for OIFR. Any use of OIFR must satisfy the requirements of the relevant Use Case and this Policy.

5.3 A subject in a potential Probe Image is a Permitted Probe Subject for the purpose of Use Case A where either:

a) The subject has been detained by a constable other than where Use Case B applies; or

b) It is reasonably suspected that the subject:

i. is wanted by the courts;

ii. has committed, is about to commit or is in the process of committing a recordable offence;

iii. is subject to bail conditions, court order or other restrictions that would be breached as a result of the context depicted in the Probe Image;

[9] The statutory powers to take a photograph at paragraphs (b) to (d) remain subject to the exercise of such power not being contrary to the interests of national security and para (a)(v) to Annex C.
[10] Reference to statutory powers under the Immigration Act 1971 reflects the legal authority to obtain a photograph. It does not, of itself, authorise the use of OIFR for wider immigration enforcement purposes falling outside this Policy.

iv. presents a risk to UK national security by officers where this assessment is undertaken or supported by officers or police staff working within Counter Terrorism Policing;

v. presents a risk to their life or an otherwise vulnerable person requiring a response to ensure their safety;

vi. is deceased, grievously injured or unresponsive.

5.4 A subject in a potential Probe Image is a Permitted Probe Subject for the purpose of Use Case B where the subject has been lawfully arrested or detained.

6 Permitted Image Reference Libraries

6.1 A Permitted Image Reference Library must be approved for use by the MPS SRO for OIFR on the adoption of this OIFR Policy and associated impact assessments which include consideration as to their use.

6.2 The following Permitted Image Reference Libraries approved for use in the OIFR System are:

a) Custody Images[11]– All OIFR Users

6.3 Any use of any Permitted Image Reference Library must comply with the rules on Images (as set out in Annexes C and D below).

6.4 **Use of the Unsolved Crime Cache**

Note: During the Proof of Concept the UCC will not be operational

6.5 The OIFR Search will also be run against the Unsolved Crime Cache for the purposes of seeking to resolve the identity of an unknown subject held in the Unsolved Crime Cache or otherwise enabling policing investigations to be linked the common unknown subject. The addition to, and retention of images in the Unsolved Crime Cache is governed by the MPS RFR Policy Document.

7 Proportionality

7.1 This Section sets out how the MPS seeks to ensure that OIFR use is proportionate.

Use Case A

7.2 Prior to undertaking any OIFR Search under Use Case A, the decision maker **must** consider whether the proposed use of the OIFR System would be a proportionate means of achieving the MPS's policing objectives, in light of the impact from the use of the OIFR System on the rights and freedoms of members of the public. If the proposed use of the OIFR System is not proportionate, the decision maker **must not** proceed to use the OIFR System as proposed, even if the proposed use would be in relation to a permitted OIFR Use Case and involve Permitted Probe Subjects and/or permitted Probe Image Reference Libraries in accordance with the requirements of this policy.

[11] Only images lawfully held by the MPS shall be included within the Custody Image Database. Inclusion in the Image Reference Library is restricted to images contained within the Custody Image Database. This includes strict adherence to MOPI requirements and all applicable MPS retention and deletion policies.

7.3 In order to consider proportionality, decision-makers should turn their minds to two key questions:

a) Is there a **less intrusive way** of effectively achieving the relevant policing objective?
b) Is the impact of OIFR **fair** on those affected?

7.4 The guidance in this section should help decision-makers understand how to answer those questions in an operational scenario. Because decisions on OIFR will be reactive and will often need to be made quickly, it is unlikely that officers will be able to refer to this guidance in real time. Therefore, officers should bear in mind the two questions above, and should ensure that they have read and familiarised themselves with this guidance on how to answer those questions, before using OIFR. All officers who are authorised to use OIFR will have completed the relevant training in advance.

Is there a less intrusive way than OIFR of effectively achieving policing objectives?

7.5 OIFR will not be the only effective way of achieving the relevant policing objectives, if there are **alternative means** of doing so, which would not substantially compromise policing effectiveness, and would have a lesser adverse impact on the fundamental rights and freedoms of potentially affected members of the public. There are two aspects to this:

(a) **Non-OIFR alternatives:** OIFR should not be used if a less intrusive policing method could be used without unacceptably compromising the achievement of the relevant policing objectives. Examples of non-OIFR alternatives include:

(i) Requesting information: for example, there may be circumstances where the subject is willing and/or required to answer questions to provide identifying details;

(ii) Pursuing other lines of investigation: for example, following up on information already known, or undertaking biographic checks not involving biometric processing (e.g. a vehicle registration check) which may resolve the identity of the subject of interest, or undertaking other index checks based on known information;

(iii) Open-source checks: seeking to process the investigation by reference to publicly available data (e.g. checking passenger lists) without the need for biometric processing;

(iv) Manual checks: if the size of the Image Reference Library is sufficiently small for such a review to be viable.

(b) **OIFR alternatives:** if OIFR is to be used, its use should be designed and deployed in a way that avoids undue interference with the rights and freedoms of members of the public. The OIFR User should consider, for example, whether the Probe Image could be acquired in a way that has a lesser impact on the subject's rights (for example, by avoiding the capture of the individual outside a place of worship).

Is the impact of OIFR fair on those affected?

7.6 To make an assessment of whether the impact of OIFR is fair on those affected (including, most obviously, the subject being searched), the officer must weigh the operational need to

deploy OIFR against the rights and freedoms of those affected by the proposed use of OIFR and the achievement of the relevant policing objectives.

7.7 An OIFR search involves the automated processing of a subject's biometric data using novel technologies. For this reason, the law treats this as a sensitive kind of processing that interferes with the subject's **right to privacy**:

(a) Officers should proceed on the basis that there is always some interference with the subject's privacy rights where (i) a person's image is ingested as part of an Image Reference Library, (ii) a person's image is used as a Probe Image to undertake an OIFR Search, and (iii) where a search result is returned and it is considered to be a Viable Match.

(b) Privacy rights may be engaged with greater intensity if the use of the OIFR System relates to images where the type of image(s) or the means by which the image(s) were captured means the public would have greater expectations of privacy. For example, the type of images where members of the public have greater expectations of privacy would be those depicting children, those with a relevant disability, images where they pre-date a person's gender reassignment, those taken in a medical context, at places of legal advice, care homes, polling stations and those in a domestic setting (see Annex D). Images where steps have been taken to ensure the images are not typically publicly available/available to the police, or where the subject is not a suspect in a criminal investigation, for example because they have been found unresponsive, are missing or are a victim, will attract particularly high expectations of privacy.

Private and/or residential premises

7.8 Where a Probe Image is obtained within residential premises, a private vehicle, or another location where an individual would reasonably have an elevated expectation of privacy, OIFR Users must have particular regard to the impact of the proposed use on the individual's Article 8 rights. OIFR Users should recognise that imagery obtained in such circumstances engages heightened privacy considerations associated with activities taking place within private spaces. The fact that a photograph is obtained within residential premises, a private vehicle, or another private location will generally weigh in favour of enhanced transparency as addressed at paragraph 12.2(d) a more detailed proportionality assessment, and careful consideration of whether the proposed use is necessary and proportionate to the legitimate aim pursued.

7.9 Depending on the circumstances, OIFR may also interfere with the subject's other rights. For example:

(a) **Freedom of thought, belief and religion** will be relevant in some cases; for instance, if Probe Images show a person wearing items of religious significance or attending a place of worship.

(b) **Freedom of expression and freedom of assembly** will be relevant in some cases; for example, if Probe Images relate to criminality at a particular protest, demonstration or other types of assembly. Decision makers should have due regard to the risk that the use of OIFR may have a chilling effect on the willingness of some individuals to take part in a lawful assembly and express their views in future, for example if the

expected use of OIFR is preannounced as an operational tactic prior to anticipated violence.

(c) **Freedom from discrimination** protects people from discrimination in the enjoyment of one or more other human rights, even where those other human rights have not been breached. Decision makers should consider whether the use of OIFR is likely to have a particular impact on one group in society, for example because of characteristics relating to their sex, race, colour, language, religion, political or other opinion or belief, national or social origin, association with a national minority, property, or birth, age, disability, gender reassignment, marital or partnership status, pregnancy or maternity, or sexual orientation.

7.10 Officers should consider the extent to which OIFR would interfere with the fundamental rights and freedoms. The more serious and extensive the interference with fundamental rights, the more that will weigh against the use of OIFR striking a fair balance.

7.11 To determine whether this is fair, officers should consider:

(a) *The degree to which the use of OIFR will enable policing objectives to be achieved*. The more effective the use of OIFR from a policing perspective, the more that weighs in favour of it striking a fair balance between competing rights and interests.

(b) *The degree to which the use of OIFR supports fundamental rights and freedoms*. In some circumstances, the public's exercise of their fundamental rights may be under threat: for example, their rights to physical integrity may be threatened by a risk to public safety, or their rights to freedom of religion may be adversely affected by a threat to a place of worship. Similarly, the use of OIFR may enable the MPS to positively contribute to upholding rights and freedoms of individuals – for example taking reasonable steps to address risks to the right to life by supporting an investigation to locate missing persons, or more effectively supporting access to medical care and other forms of support for the grievously injured and victims of crime.

(c) *How the use of OIFR compares to any non-OIFR alternatives.* If the use of OIFR would make a significantly greater contribution to achieving the policing aim than non-OIFR alternatives (for example, because the alternatives would be significantly more resource-intensive), then that will weigh in favour of the use of OIFR striking a fair balance.

7.12 Even if OIFR is the only effective way of achieving a policing objective, it will not be proportionate if it does not strike a fair balance between competing rights and interests. In such circumstances, it must not be used.

Use Case B

7.13 The MPS considers the use of OIFR under Use Case B to be a proportionate means of supporting the safe, lawful and effective management of arrested or otherwise detained persons.

(a) Individuals entering police detention may present with a range of risks and vulnerabilities, including risks of violence, self-harm, suicide, mental ill-health, substance misuse, safeguarding concerns and medical needs. Effective custody management depends upon the ability of officers and staff to identify and appropriately manage those risks. The importance of robust risk identification and management within custody has been recognised by HMICFRS, whose 2025 inspection of MPS custody facilities identified risk management, safeguarding and detainee welfare as critical aspects of custody operations.

(b) The custody environment also presents risks to police officers and staff. Between 1 October 2025 and 30 September 2026, the MPS recorded 1,036 assaults on officers and staff occurring during custody procedures within custody facilities. Of those incidents, 782 (75.5%) occurred within police cells, charge desks and cell wings. These figures demonstrate that custody environments involve exposure to violence and disorder and that identifying relevant risk information has a legitimate and important operational purpose to ensure an efficient, effective and safe custody environment.

(c) The safe management of detained persons depends upon access to accurate information concerning their identity and associated risk profile. Relevant information may be recorded against an individual's true identity, aliases or linked identities and may include warning markers, violence indicators, self-harm history, medical information, safeguarding concerns and other information relevant to detainee care and officer safety. Experience within policing demonstrates that detained persons do not always provide accurate identifying information and may provide false, incomplete or inconsistent biographical details. By its nature, the prevalence of undisclosed aliases and false identities cannot readily be quantified, as successful deception may go undetected. In other cases, a detained person may be unable to provide reliable identifying information due to intoxication, physical injury, mental ill-health, vulnerability, language difficulties or other communication barriers. As a result, searches conducted solely using biographical information may fail to identify information necessary for the safe and effective management of the detainee. Accurate identification is particularly important within custody and other detention environments, where officers and staff are required to make decisions concerning detainee welfare, safeguarding, healthcare, observation levels and risk management, and where establishing a subject's true identity may reveal risks, warning markers, outstanding warrants, links to unresolved offending or other information that would not otherwise be apparent from the details provided by the detainee.

7.14 It is not reasonably possible for officers to know, in any particular case, whether an OIFR search will reveal information that enables the safe management of arrested or otherwise detained persons. For example, it will not be possible to know whether a subject has aliases that they have not shared with officers, such that searching them by name would be ineffective.

7.15 Under Use Case B, OIFR will be used in all cases where the conditions under paragraph 2.7 above are met. Accordingly, members of the Metropolitan Police Service are not expected to conduct a case-specific proportionality assessment when using OIFR under Use Case B (and

many of the specific factors set out above would not be relevant under Use Case B in any event).

8 Use of the OIFR System

Pre-Requisites to an OIFR Search

8.1 Under Use Case A, the OIFR Submission Form must record that non-OIFR alternatives have been considered and are exhausted, are otherwise considered unviable in the circumstances, or that the use of OIFR is justified by Urgency (for example in circumstances where there is an imminent threat to life).

OIFR Submission Form

8.2 Every Permitted Probe Image submitted for OIFR Searching will need to be supported by an OIFR Submission Form, completed by the OIFR User to confirm the OIFR Search is being undertaken in compliance with the requirements of this Policy as summarised at paragraph 1.3.

8.3 The following require the OIFR Submission Form to be supported by an approval from an officer of inspecting rank (or above) or staff equivalent:

a) The use of any Imagery (as a Permitted Probe Image, or Permitted Image Library) assessed to be at Level 4 or 5 in the Imagery Matrix at Annex C[12];

b) Where required as a specific safeguard as set out in the table at paragraph (f) to Annex D: Imagery and Protected Characteristics.

8.4 Where, due to circumstances of Urgency, it is not practicable to complete an OIFR Submission Form before a search without materially negatively impacting on the operational need to conduct an OIFR search,

a) An OIFR Submission Form may be completed as soon as practicable after the search has taken place; and

b) For a search requiring approval from an officer of inspecting rank, that permission may be given and sought orally prior to the search. As soon as practicable after the search has taken place, the officer of at least the rank of Inspector shall record on an OIFR Submission Form that oral permission was granted and set out the reasons with which he was provided to justify the authorisation.

8.5 **Ingesting imagery**: The process of how to ingest imagery into the MPS OIFR system is set out in the MPS Reveal Training Guide (pages 35 – 43 detail how to upload images to a case).

8.6 **Face detection**: The OIFR Search system includes a progressive search function designed to embed privacy by design principles, minimising unnecessary data processing and intrusion

[12] For the purposes of this paragraph, imagery obtained pursuant to Use Case A within residential premises, a private vehicle, or another location attracting heightened expectations of privacy will ordinarily be treated as Level 4 imagery unless a higher classification applies.

where images contain multiple faces. When a Permitted Probe Image is submitted, the system will, where practicable, first detect any faces present in the image. Only those faces selected by the OIFR user will then be subjected to OIFR searching, for which Potential Matches may be returned for adjudication. Only the faces of Permitted Probe Subjects, as specified in the OIFR Submission Form, should be selected for OIFR searching.

Adjudication and results

8.7 When an OIFR search is undertaken, any Potential Match identified by the OIFR System may be returned to the OIFR User for review and adjudication. Potential Matches are presented in ranked order according to similarity score, with the highest ranked result presented as rank one[13]. The absence of a returned result does not establish or confirm identity.

8.8 It is for the OIFR User to Adjudicate the results and determine whether any Potential Match is a Viable Match. OIFR Users must not assume that a Potential Match (highly ranked or otherwise[14]) is a Viable Match but must undertake their own independent consideration of whether a Potential Match is a Viable Match. In considering a Potential Match, the OIFR User must give due regard to Subject[15], System or Environmental Factors and the impact that they may have on the likelihood that any Potential Match is a Viable Match.

8.9 **Match Report:** The OIFR User must complete a Match Report, this is embedded with the OIFR System.

8.10 The Match Report must:

a) Confirm the Potential Match relates to the policing objective underpinning the Use Case.

b) Record whether the OIFR User has determined the Potential Match to be a Viable Match or not. A Match Report must be completed in all cases, including where the Potential Match is assessed not to be a Viable Match, for audit purposes.

c) Where a Potential Match is assessed to be a Viable Match:

i. provide a rationale explaining why the OIFR User considers the images to depict the same individual, noting any specific facial or distinguishing features relied upon;

ii. confirm that, in reaching that assessment, the OIFR User has considered, where relevant:

1. the quality of the probe image;

[13] Only the Rank One Potential Match shall be displayed to officers conducting an OIFR Search using an MPS Device.

[14] This is the case where the OIFR User is completing an OIFR Search on a MPS Device whereby only rank one results are returned.

[15] Some Subject Factors may be linked to protected characteristics. Those undertaking the Adjudication are best placed to consider the impact of any factors which may have influenced the OIFR system when it generated a Potential OIFR Match and if such factors combine to mean that proceeding to a Match Report is not appropriate in the circumstances. Examples include, a head covering worn as an act of thought, conscious or religion, those with a relevant disability such as a facial disfigurement or those who have changed their sexual orientation and undergone surgery changing their facial appearance.

2. the quality of the images within the Image Reference Library;
3. the time elapsed between the capture of the Image Reference Library image and the Probe Image;
4. lighting conditions e.g. poor lighting/shadow; and
5. other subject, system and environmental factors which might impact on the performance of the OIFR System and the viability of the match,

and must record which (if any) of these factors were material to the assessment in the particular case.

8.11 If the OIFR User determines that there is a Viable Match, the Match Report should in the case of an outstanding criminal investigation, be included within the Crime report and investigative material.

8.12 A determination that a Viable Match exists does not, of itself, establish identity and must be considered together with all other available information and evidence.

Dissemination

8.13 Dissemination beyond the MPS is not anticipated. In the event the OIFR User establishes a need to share the results of an OIFR Check, the OIFR User should consider whether advice should be obtained from the Directorate of Legal Services, the Data Protection Officer (or someone on their behalf from the Data Office) and the MPS FRT team.

Use of results

8.14 Where the OIFR User has determined that there is a Viable Match, this must not to be treated as a definitive confirmation of identity for evidential purposes. It is an intelligence lead only.

8.15 Subject to paragraph 8.14 and not unlike other circumstances where officers receive a description they recognise to be a suspect, or manually compare two images and determine them to be of the same person, a constable is entitled, following receipt of a Viable Match, to take into account that Viable Match as to whether they suspect or believe that the subject is a particular individual. A Viable Match may therefore support immediate operational decision making, including the decision to act or not. However, the OIFR User must:

a) not solely rely on the existence of the Viable Match.
b) be able to articulate and justify the use of any powers or operational response;
c) ensure that any action taken must have a clear lawful basis.
d) ensure that any action is necessary and proportionate in the circumstances.

8.16 Depending on the circumstances, and the OIFR Users assessment of the threat, harm and risk, proportionate responses to a Viable Match may include:

e) intelligence checks (for example using PNC) as a result of having an identity or other information search against (for example against a vehicle registration number);

f) corroboration with other information held in relation to the investigation (for example to establish if known marks, scars or tattoos are present);

g) asking the subject for further information;

h) undertaking open-source checks now made possible as a result of the Viable Match;

i) the utilisation of other policing powers.

8.17 OIFR does not confer any additional power to stop, question, detain or arrest an individual. Any engagement with an individual must be supported by an applicable legal power or lawful policing purpose. Absent any applicable statutory powers arising, officers may use their common law powers to, for example, ask questions to advance an investigation or operation. This may be particularly applicable where an individual is not sought on suspicion of an offence or with a warrant for their arrest outstanding but, for example, because the MPS is seeking to determine compliance with conditions imposed on a person under a Court Order. Officers must comply with the Code of Ethics and the National Decision Making Model at all times.

8.18 A subject's refusal to participate in an OIFR process under Use Case A does not, in isolation, provide sufficient grounds for arrest or detention. However, it may, depending on the circumstances, be one of the matters relevant to the officer's consideration of whether the legal criteria for arrest or detention are satisfied.

Disclosure considerations

8.19 The SIO/OIC remains responsible for matters considering disclosure in their case. The SIO/OIC should consider whether the Match Report is disclosable in their case.

9 Audit and reporting

9.1 The OIFR System provides a web-based administration client that includes both real-time and historical reporting on system usage and performance. Structured reports on historical usage can be run from within the solution or scheduled for delivery on a periodic (hourly, daily, monthly) basis to specified administrators.

9.2 Audit log data are stored in a read-only database, ensuring that once written, data cannot be modified. Access to review audit data is provided as part of a separate web-based administrative client and only granted to authorised users through the integrated Role Based Access Control (RBAC). Audit log data, together with the OIFR Submission Form and the Match Report, support the MPS's compliance with the accountability and record-keeping requirements under section 62 of the Data Protection Act 2018.

9.3 All actions on audit data, including queries and individual item reviews, are also audited as part of the application activity, ensuring full tracking of all data and access within the system.

10 Governance and oversight

10.1 The following documents and this Policy together comprise the MPS OIFR Documents which govern the use of the MPS OIFR System:

a) MPS OIFR Data Protection Impact Assessment (DPIA);

b) MPS OIFR Appropriate Policy Document;

c) MPS OIFR Equalities Impact Assessment (EIA);

d) MPS Facial Recognition Technology: Understanding accuracy and demographic differences;

e) MPS OIFR Legal Mandate; and

f) MPS Training Guide and NEC Training materials

10.2 The MPS OIFR Documents are further implemented:

a) in terms of the use of Image Reference Libraries and Probe Images by:

b) the SRO for OIFR approving the use of Permitted Image Reference Libraries by the adoption of this Policy;

c) the completion of the OIFR submission form authorising the OIFR Search per paragraph 8.2 – 8.4 of this Policy.

10.3 **Authorised OIFR Users:** All users of the OIFR Systems will have completed the requisite training for the role they are required to perform.

10.4 Access to the OIFR system is strictly managed by a limited number of staff who have specialist administrator rights. System usage will be monitored and access rights disabled (or removed) if it is assessed that any user no longer requires use of the system[16].

10.5 **Oversight:** Within the MPS, the senior responsible officer (SRO) for facial recognition is responsible for the strategic direction of OIFR. Internal oversight for OIFR is provided through the MPS FR Technology Board, which in-turn answers to the MPS Management Board. The MPS FR Technology Board is charged with reviewing the use of OIFR on an at least quarterly frequency to monitor for trends and direct changes for best practice. The MPS FR Technology Board will also consider aggregated demographic data relating to OIFR Searches at these meetings and take steps as required to ensure the MPS continues to discharge is PSED responsibilities.

10.6 In addition, MOPAC provide oversight and scrutiny while the London Policing Ethics Panel (LPEP) provide independent insight and guidance. Lastly, other regulatory bodies, including Surveillance Camera Commissioner (SCC); Biometrics Commissioner (BC), the Information Commissioner's Office (ICO) and Equality and Human Rights Commissioner (EHRC) provide independent reviews and consultation.

11 Data management

11.1 The MPS must ensure that the processing of any data by the OIFR system is conducted in a lawful way and in compliance with the MPS OIFR Documents. This means that:

(a) Information pertaining to the submission and searching of Probe Images and the use of Image Reference Libraries (including the image, associated biometric image template, and meta data relating to that image e.g. crime type) will be retained:

[16] During the Proof of Concept phase, only 100 MPS officers shall use the OIFR system for operational purposes.

i. in accordance with the Data Protection Act 2018, MOPI, the Criminal Procedures and Investigations Act 1996; and / or

ii. personal data is retained in accordance with the MPS's complaints / conduct investigation policies.

(b) The above provisions represent upper limits. In line with MOPI there is a need for consideration as to the case for retention in the circumstances surrounding the OIFR Search, and if elevated expectations of privacy apply such that a lower retention period should be adopted. In this vein, and to support officers and ensure consistent decision making in certain areas, the following additional safeguards apply:

i. In relation to different age groups and having regard to the currency of images for an OIFR Search, the following additional provisions apply when interpreting MOPI in relation to the retention of data in the OIFR System:

<table>
<tr><th colspan="2">Subject age</th><th>MOPI 3</th><th>MOPI 2</th><th>MOPI 1</th></tr>
<tr><td>Under 13 years old</td><td>Image Reference Library</td><td>Not in scope for OIFR Searching</td><td>Not in scope for OIFR Searching</td><td>Not in scope for OIFR Searching</td></tr>
<tr><td>13 – 15 years old</td><td>Image Reference Library</td><td rowspan="2"></td><td rowspan="3">Up to 10 years from image capture</td><td rowspan="3">Up to 10 years from image capture</td></tr>
<tr><td>16 – 18 years old</td><td>Image Reference Library</td><td>Up to 3 years from image capture</td></tr>
<tr><td>Over 18</td><td>Image Reference Library</td><td>Up to 6 years from image capture</td></tr>
</table>

ii. In relation to Probe Images where a Viable Match is returned, the purpose for the OIFR Search has been completed and subject to paragraph 11.1 concerning disclosure obligations as they may arise, the Probe Image is no longer required in the OIFR System and as a result deletion will occur within 31 days of the OIFR Search.

iii. In relation to Probe Images, where a Viable Match is not returned:

A. Unsolved Crime Cache: there is a requirement to remove the Probe Image where the policing purpose has been resolved by other means. Personnel will additionally be required to review Probe Images in OIFR System every 3 months for Tier 3 offences, 6 months for Tier 2 and 9 months for Tier 1 after submission to ensure the continuing need for the OIFR Search and that the OIFR Search continues to satisfy this policy. The Tiers are set out in Annex C and have themselves been subject to a DPIA assessment as part of the FIMS facial library DPIA.

B. Where no further OIFR Searching is required, deletion from the OIFR System will occur within 31 days of the OIFR Search.

12 Transparency

12.1 **Policy and documentation**

(a) The MPS makes this policy, the associated impact assessments and wider information available to the public on its website.

12.2 **During use**

(a) Where a statutory power provides the legal basis for the taking and/or use of a photograph, the OIFR User must act in accordance with that power and comply with any applicable Code of Practice.[17] Where compliance with paragraph 12.2(b) would impose additional requirements that are not inconsistent with that power or Code of Practice, those requirements must also be followed.

(b) In all other cases, the OIFR User should inform the subject of:

(i) the purpose of taking the photograph and the use to which it is to be put (the Use Case)

(ii) the grounds on which the photograph is being taken (the basis upon which the person is considered a Permitted Probe Subject)

(iii) that the photograph will be used for OIFR searching..

(c) When seeking to inform a subject in accordance with paragraph 12.2(b), OIFR Users should, wherever reasonably practicable, provide that information before image capture.

(d) Where a photograph is to be obtained pursuant to Use Case A within residential premises or a private vehicle the information set out at paragraph 12.2(b) must be provided **before** image capture. OIFR must not be used in such circumstances unless the subject has first been provided with that information.

(e) In all other circumstances, where it is not reasonably practicable to provide the information set out at paragraph 12.2(b) before the photograph is taken because:

(i) the photograph is being captured as an immediate reaction to events and any delay would result in the loss of the opportunity to obtain it; and/or

(ii) the OIFR User reasonably believes that providing the information would result in an unacceptable risk to themselves or others (including the Permitted Probe Subject); and/or

(iii) the Permitted Probe Subject lacks the capacity to understand the information at the time because they are deceased, grievously injured or unresponsive,

then, the OIFR User must, where reasonably practicable, ensure that the Permitted Probe Subject is provided with the information set out at paragraph 12.2(b) as soon

[17] For example, PACE Code D and the Codes of practice for officers using examination powers at ports.

as practicable after the photograph has been taken and create a record of that information having been provided to the Permitted Probe Subject.

(f) Where the Permitted Probe Subject is a child or has another protected characteristic which may impact on understanding, OIFR Users must ensure that all communications are clear, age-appropriate, and capable of being understood in so far as is reasonably practicable. Training and guidance provided to OIFR Users shall address the requirements of appropriate and accessible communication with Permitted Probe Subjects. This shall include consideration of the needs of the individual and any relevant protected characteristics including those who may have communication, cognitive, or language needs, so as to ensure information is conveyed clearly and in a manner capable of being understood.

(g) Where OIFR is used and Body Worn Video is required to be worn, it should ordinarily be activated in accordance with MPS Body Worn Video policy and applicable legal requirements. The use of Body Worn Video provides an important transparency and accountability safeguard in relation to the use of OIFR.

12.3 **Wider information**

(a) On an annual basis, the MPS will provide a report on its use of OIFR including how it has been used and the results gained. The report will also provide demographic analysis relating to OIFR searches undertaken.

(b) The MPS is responsive to requests made under the Freedom of Information Act 2000, or in relation to the exercise of individual rights pursuant to the Data Protection Act 2018. The published MPS Privacy Policy contains further details as to how individual rights may be exercised.

Annex A: Terminology

Adjudication	means a human assessment of a Potential Match generated by the OIFR System to determine if the Potential Match should be considered to be a Viable Match or not.
Biometric Template or Template	is 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. Note that Templates are proprietary to each facial recognition algorithm and new Templates will need to be generated from the original images if the algorithm is changed.
Environmental Factor	is an external element that may affect RFR system performance such as dim lighting, glare etc. in the images.
Facial Recognition (FR)	is a technology which 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 possible matches.
Match Report	means the record completed by an OIFR User following the determination that a Potential Match constitutes a Viable Match.
OIFR	means the use of the MPS OIFR System whereby an OIFR User submits a specifically selected Probe Image for comparison against a Substantive Image Reference Library in support of a Permitted Use Case.
OIFR Search / OIFR Searching	means the use of the OIFR System to compare a Probe Image against a Permitted Image Reference Library in order to identify Potential Matches.
OIFR Submission Form	means the form to be completed by an OIFR User undertaking a search or by the person tasking the OIFR User to initiate a OIFR Search.
OIFR System	means the OIFR Neo Face Reveal facial recognition system as used by the MPS.
Permitted Probe Subject	means a person who satisfies the requirements of section 5 of this Policy and whose image may be used as a Probe Image for the purposes of an OIFR Search.
Permitted Use Case	means a use of OIFR authorised by section 2 of this Policy.
Permitted Image Reference Library	has the meaning given to it in section 6 of this Policy.
OIFR User	means an authorised user of the MPS OIFR System.
Potential match	means a result generated by the OIFR System following a comparison between a Probe Image and an image within the Substantive Image Reference Library, based on a similarity score, and presented to an OIFR User for Adjudication. A Potential Match does not in itself confirm identity and must not be treated as a Viable Match unless and until it has been assessed by an OIFR User.
Probe Image	means a single still image depicting a Permitted Probe Subject, which is specifically selected and submitted by an OIFR User to the OIFR System for the purposes of undertaking an OIFR Search in accordance with this Policy.
Rank-one	means the highest-ranked Potential Match returned by the OIFR System following an OIFR Search, based on the highest similarity score generated by the system when comparing the Probe Image against a Permitted Image Reference Library.

Subject Factor	means a factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time the photograph was taken.
System Factor	means a factor relating to the OIFR system and how it performs such as the algorithm, the passage of time since Permitted Probe Image was taken, the quality/resolution/clarity of the image taken.
Tiers	means the tiers of offences referred to in Annex C of this RFR Policy which are used to determine the retention of images within the Unsolved Crime Cache (when this searching is activated).
Unsolved Crime Cache	is a distinct collection of images where a Permitted OIFR Use Case continues to exist in relation to a Permitted Probe Subject following an initial OIFR Search.
Urgency	Urgency means: a) an imminent threat to life or an imminent risk of serious harm to a person or property; and/or b) a time-critical operational or investigative opportunity where delaying action to comply with ordinary approval or administrative requirements would materially prejudice the achievement of the relevant policing objective.
Viable Match	means a Potential Match, where following Adjudication, the OIFR User has determined that the Potential Match depicts the same individual as the Probe Image.

Annex B: Types of FR

<table>
<tr><th colspan="4">FACIAL RECOGNITION OVERVIEW</th></tr>
<tr><td colspan="2">Facial Recognition – Method of use:</td><td>The use of facial recognition where all people passing the system's camera(s) are analysed by the system with results being generated at the same time as events.</td><td>The use of facial recognition where:
(i) media is directly captured of a subject present; or
(ii) media is otherwise acquired in lieu of capturing it,
with the intent of subjecting it to analysis by the facial recognition system.</td><td>The use of facial recognition where media is analysed after the event. The result of such analysis would come sufficiently after the event such that they could not shape events to which the media related in real time.</td></tr>
<tr><td rowspan="2">Overt</td><td>Name</td><td>Live Facial Recognition (LFR)</td><td>Operator Initiated Facial Recognition (OIFR)</td><td>Retrospective Facial Recognition (RFR)</td></tr>
<tr><td>How it may be referred to:</td><td>"... the use of overt live facial recognition to locate people on a watch list who are sought by the police …"</td><td>"... the use of operator initiated facial recognition which takes an image of a particular person and uses it to either (i) help policing establish who a person in the image is or (ii) establish where a person has previously appeared in other media held by the police ..."</td><td>"… retrospective facial recognition may be used after an event to help officers establish who a person is or whether their image matches against other media held on databases ... "</td></tr>
<tr><td rowspan="2">Covert</td><td>Name</td><td>Covert Real-Time Facial Recognition Surveillance (CRFRS)</td><td>Covert Operator Initiated Facial Recognition Surveillance (COIFRS)</td><td rowspan="2">RFR is not a covert capability in itself. It may however use media obtained via covert means.</td></tr>
<tr><td>How it may be referred to:</td><td colspan="2">… "whilst the then Surveillance Camera Commissioner has recognised a possible application for facial recognition in a covert way, subject to the Regulation of Investigatory Powers Act 2000, policing does not comment on any potential use of covert policing tactics …"</td></tr>
</table>

Annex C: Imagery

(a) Images must only be used for OIFR searching where the MPS is reasonably satisfied that the image:

(i) has been lawfully captured and is lawfully held by the MPS[18];
(ii) is of a suitable quality for OIFR searching having regard to the prospect of the system returning a viable match (see Section 8);
(iii) is held by the MPS in a format which allows it to be used for OIFR searching;
(iv) is of a government security marking suitable for use in the OIFR system;
(v) is capable of use within the OIFR System without giving rise to any national security risk, having regard to the classification of the OIFR System, whether such risk arises from the record in isolation or from its aggregation with records obtained through OIFR Searching;
(vi) of the images that meet criteria (i)-(vi) above, has been taken in a way which seeks to reflect the lowest privacy and human rights expectations attached to it in line with paragraph (e) of this Annex.

(b) The OIFR System is capable of ingestion of still images,– this is not a capability that provides an option for users seeking to undertake mass video analysis.

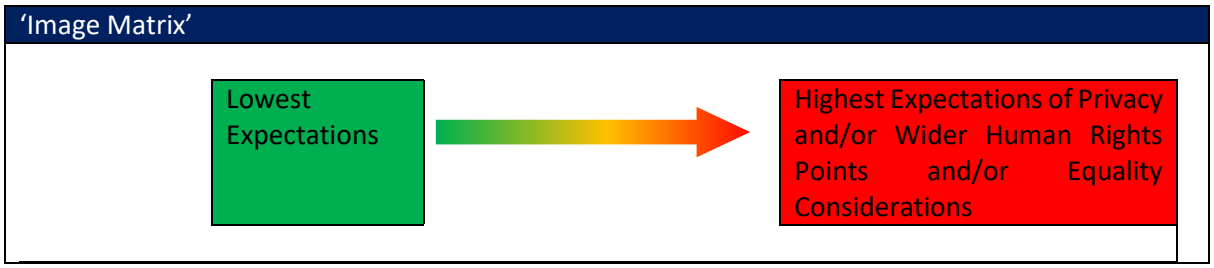
Image quality

(c) To ensure the MPS is reasonably satisfied that an image is of a suitable quality for OIFR searching having regard to the prospect of the OIFR System returning a viable match, the OIFR System assesses images for searching to ensure they are of suitable minimum quality and indicates those that may pose issues to the OIFR User for a resolution.

(d) The OIFR User is trained on, and required to consider the impact on Subject, System and Environmental Factors when determining the viability of any match (see Section 8).

Sources of imagery

(e) Where it is necessary to assess the expectations of privacy attaching to a Probe Image or Image Reference Library, decision makers should use the matrix below. Any doubt as to the correct Level should be resolved in favour of the higher Level.



[18] The MPS has a number of powers that allow it to capture images, including those set out at paragraph 4.3 of this Policy. Where there are specific requirements regarding the capture of images, including in applicable Codes of Practice, these must be complied with, in addition to the requirements of this Policy.



Image Level	Description	Example(s)
Level 1	Police-originated Probe Images / Image Reference Libraries which contain a majority of images obtained: • in compliant circumstances where reasonable steps have been taken to ensure the subject was aware that their image was taken; or • the subject of the image is deceased.	• An image taken of a compliant subject in the custody environment. • An image taken during an interaction with policing where the subject for OIFR Searching is compliant with policing.
Level 2	Police-originated Probe Images / Image Reference Libraries which contain a majority of images obtained in non-compliant circumstances where reasonable steps have been taken to ensure the subject was nevertheless aware that their image was taken.	• An image taken of a non-compliant subject in the custody environment. • Police controlled overt CCTV • An image taken during an interaction with policing where the subject for OIFR Searching is not compliant with policing
Level 3[19]	Non-police originated Probe Images / Image Reference Libraries which contain a majority of images where it is assessed that the public would expect law enforcement to have access to them (but not including images obtained by covert means).	• Local authority or other third party controlled overt CCTV shared with policing.

[19] Not relevant for OIFR.

Image Level	Description	Example(s)
Level 4	Probe Images / Image Reference Libraries which contain a majority of images where it is assessed that they: • raise elevated privacy expectations; • raise wider human rights issues; • raise equality considerations as a result having a particular impact on those with a protected characteristic; and/or • where the images were otherwise obtained covertly without the knowledge of the subject but where the ability of the police to obtain such images can be anticipated by reference to published Codes of Practice.	• Imagery obtained pursuant to Section 64A of the Police and Criminal Evidence Act 1984 (until such point as the subject has been informed that the image has been taken where such action is required by PACE Code D); • Imagery obtained via the Regulation of Investigatory Powers Act or the Investigatory Powers Act 2016. • Images which are more sensitive because they were taken at hospitals, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), care homes, feature persons at a lawful assembly or those taken in a domestic setting.
Level 5[20]	Non-police originated Probe Images / Image Reference Libraries which contain a majority of images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessibly by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received.	• Where the public have shared their image with a controller of data for an explicit purpose and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This may be particularly relevant with businesses who promote their privacy-lead approach and take active steps to prevent any form of third party access.

(f) In line with the matrix above, where it is viable to do so without unduly impacting on the performance of the OIFR System and the objectives of undertaking an OIFR Search, suitable, compliant police-originated images should be preferred for OIFR Searching. These images have the lowest expectations of privacy and have the highest levels of foreseeability in terms of their use by the MPS.

[20] Not relevant for OIFR.

Annex D: Imagery and Protected Characteristics

(a) The MPS recognises that regardless of any performance considerations of the OIFR system, there is a need to take particular care when considering (i) age (including the protection of children – particularly the very young), (ii) those with a relevant disability[21] and (iii) those who have and/or are undertaking a gender reassignment[22]. This is because:

(i) There may be different privacy expectations around the use of OIFR[23] and that these can be particularly relevant in relation to these people given their potential vulnerability[24].

(ii) The MPS recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.

(b) Specific safeguards relating to protected characteristics and the use of Probe Images can be found at Annex D, paragraph (f) to this policy. The OIFR User must not undertake an OIFR Search without being reasonably satisfied that these specific safeguards will be implemented.

Recording composition of Probe Images

(c) OIFR Users submitting single Probe Images for searching are required to record whether person(s) contained within the Probe Image is reasonably suspected to be:

(i) aged under 18-years old;

(ii) aged under 16-years (but older than 13 years) old;

(iii) a person with a relevant disability;

(iv) a person who has undertaken a gender reassignment and it is reasonably suspected that the Probe Image is of an image of the person taken prior to their reassignment.

---

[21] A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) and that such a disability may impact on the performance of the police force's OIFR system. Examples which may have an impact (depending on the performance characteristics of the specific OIFR system) include if the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised.

[22] In this context means those with who had and/or are undertaking gender reassignment (as the term is defined in section 7(1) of the Equality Act 2010) and that the gender reassignment may impact on the performance of the police force's OIFR system. This is more likely where a less recently taken Probe Image is being considered such that it would pre-date corresponding images in an Image Reference Library.

[23] For example, in relation to gender reassignment, see Section 22 of the Gender Recognition Act 2004 which protects disclosures other than in certain specific circumstances which include where the disclosure is necessary for the purposes of preventing or investigating crime.

[24] For example, in relation to children, see: **https://www.app.college.police.uk/app-content/detention-and-custody-2/detainee-care/children-and-young-persons/#children-and-young-persons** which is in the context of detention and custody but notes children and young people are a protected group with specific vulnerabilities. Their treatment in detention is governed not only by domestic legislation but also by the **UN Convention on the Rights of the Child (UNCRC)**;

(d) Insofar as the data is extractable from MPS systems by automated means, the MPS must also maintain a record of composition (i) sex (ii) race- by reference to IC code and (iii) age range of its Image Reference Libraries.

(e) The data relating to Probe Images and Image Reference Libraries will then be recorded in an aggregated manner to be presented to the FR Technology Board on a quarterly basis for review. Information relating to composition will be published annually in line with paragraph 12.3(a) of this Policy.

Specific safeguards

(f) The following outlines further, specific safeguards that apply to the use of Probe Images:

<table>
<tr><th></th><th>Age
(U. 18)</th><th>Age
(U.16)</th><th>Age
(U.13)</th><th>Disability</th><th>Gender
Reassignment</th></tr>
<tr><td colspan="6">Circumstances relating to the Probe Image where the subject is reasonable suspected to:</td></tr>
<tr><td></td><td>Be aged under 18 at the time of the OIFR Search.</td><td>Be aged under 16 at the time of the OIFR Search.</td><td>Be aged under 13 at the time of the OIFR Search.</td><td>Have a relevant disability</td><td>Be a case where the Probe Image pre-dates the undergoing or completion of a gender reassignment</td></tr>
<tr><td colspan="6">Additional safeguards</td></tr>
<tr><td rowspan="2">Approval</td><td>OIFR User</td><td>OIFR Search request requires approval by Inspecting rank or higher</td><td>No authority shall be provided to take image for Under 13’s</td><td colspan="2">The above categories must be approved by an officer of at least Inspecting rank.</td></tr>
<tr><td colspan="5">Approval by an officer of at least Inspecting rank is also required, in accordance with the Image Matrix at Annex C, in any case where the proposed use of the OIFR System raises equality considerations due to a particular impact on a protected characteristic</td></tr>
<tr><td>Specific Advice</td><td colspan="2"></td><td colspan="3">Where viable in the circumstances, specific advice must be sought from the MPS Facial Recognition Technology team on technical matters and, where they consider it appropriate, from the Directorate of Legal Services. Where approval is required, such advice must be made available to inform decision-making.</td></tr>
</table>

Offence limits[25]	Any offence	Recordable Offences, as defined in PACE 1984	Public protection matters[26].	
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with the MPS OIFR Documents with a particular focus on ensuring the necessity case is fully made out.			
Image	There is a particular need to ensure that the image is a current as possible and of a suitable quality for use as a Probe Image.			
		Additional controls on retention apply – see Section 11 of this Policy		

[25] Applicable to paragraph 4.1(b)ii and (b)iii

[26] MOPI Group 1.

Annex E: Proof of Concept

Proof of Concept

(a) The Metropolitan Police Service will initially deploy OIFR as a Proof of Concept to evaluate the operational utility, effectiveness, legality and proportionality of the capability in a controlled policing environment. The Proof of Concept is intended to assess whether OIFR supports the identification of individuals and the management of risk in accordance with the Permitted Use Cases set out in this Policy, whilst testing the effectiveness of the safeguards, governance arrangements, training requirements and technical performance of the system. The Proof of Concept will be subject to ongoing monitoring, audit and evaluation, including consideration of privacy, equality and human rights impacts, user compliance, operational outcomes and public confidence. The findings of the Proof of Concept will inform any decision on whether OIFR should be retained, expanded, modified or discontinued by the MPS.

Performance monitoring

(b) The OIFR Pilot will be subject to ongoing monitoring, review and evaluation to assess:
- (i) whether OIFR delivers operational benefits consistent with the Permitted Use Cases set out in this Policy;
- (ii) whether OIFR is being used in a lawful, necessary and proportionate manner;
- (iii) whether the safeguards contained within this Policy are operating effectively;
- (iv) whether any disproportionate impacts arise in practice; and
- (v) whether OIFR should be continued, modified, expanded, restricted or discontinued.

(c) The evaluation of the OIFR Pilot shall be evidence-based and aims to take account of:
- (i) operational effectiveness;
- (ii) privacy, equality and human rights impacts;
- (iii) compliance with this Policy and associated OIFR Documents;
- (iv) system performance and limitations;
- (v) user compliance and training outcomes; and
- (vi) public confidence and accountability considerations.

(d) The MPS shall maintain performance information relating to the use of OIFR, including:
- (i) the number of OIFR Searches undertaken;
- (ii) the applicable Use Case;
- (iii) the number of Potential Matches returned;
- (iv) the number of Viable Matches identified;
- (v) examples of operational outcomes arising from Viable Matches, including where they contributed to identifying an unknown subject, locating a wanted person, managing risk, safeguarding vulnerable persons, or advancing an investigation;
- (vi) examples of the extent to which OIFR provided information not otherwise obtainable through less intrusive means;
- (vii) examples of the extent to which OIFR reduced delays in establishing identity or assessing risk; and
- (viii) examples demonstrating the operational value and limitations of OIFR

(e) The MPS plans to monitor the operation of OIFR for evidence of disproportionate impact or unintended bias. Such monitoring should include, so far as reasonably practicable:

(i) demographic information relating to Probe Images and Image Reference Libraries together with overall search volumes;
(ii) consideration of protected characteristics identified within Annex D;
(iii) review of any complaints, conduct matters or legal challenges alleging discrimination or unfair treatment; and
(iv) review of any material differences in system performance identified through testing, operational deployment and technical evaluation of results

(f) The MPS plans to monitor compliance with this Policy through audit and oversight processes, including consideration of:

(i) completion and quality of OIFR Submission Forms;
(ii) compliance with authorisation requirements;
(iii) compliance with transparency requirements;
(iv) compliance with retention and deletion requirements;
(v) compliance with training and accreditation requirements;
(vi) use of OIFR in heightened privacy settings; and
(vii) any instances of misuse, error, policy deviation or technical failure.

(g) Evaluation findings shall be reported to the MPS Facial Recognition Technology Board with the outcome of the pilot to be published on the MPS website.

Data retention

(h) For the duration of the PoC, data generated through OIFR searches will be retained to enable testing, evaluation and performance analysis. Following the conclusion of the PoC, this data will continue to be retained for a maximum period of 30 days to allow for final reporting, validation and audit activities, after which it will be securely deleted in accordance with applicable data management and retention requirements. Access to the retained data will be strictly limited to a small number of authorised members of the project and IT support teams who require access for system administration, monitoring, testing and evaluation purpose

Pilot Limitations and Operational Constraints

(i) During the Proof of Concept, the Unsolved Crime Cache will not be operational and no OIFR Searches will be undertaken against it. References elsewhere in this Policy to the Unsolved Crime Cache reflect intended future functionality only and do not form part of the Proof of Concept. Prior to use, this Policy would be updated and published on the MPS Website.

(j) During the Proof of Concept, Use Case B will not necessarily be used in every instance where a statutory power exists to obtain a photograph. Its use will remain subject to operational considerations, including operational demand and competing priorities to deliver the pilot and wider FR requirements, the availability of suitably trained and authorised OIFR Users, the classification at which the system operates, technical availability, the availability of equipment, and the ability to integrate OIFR into the operational processes of a particular custody suite, detention facility or examination environment.

(k) The OIFR Proof of Concept will operate for an initial period of six months.

(l) The governance arrangements, evaluation methodology and this Policy will be kept under review throughout the Proof of Concept and may be amended where necessary to reflect operational learning, legal developments or assurance requirements.