More Trust | Less Crime | High Standards

DATA PROTECTION APPROPRIATE POLICY DOCUMENT

(APD)

1 Executive summary 3

2 Description of Data Processing.....3

3 Consent or Schedule 8 Grounds for Processing.....7

4 Procedures for ensuring compliance with the principles.....8

5 Policy applicable to retention and erasure 13

6 Protective Marking.....14

Terms & Definitions: Capitalised terms used in this MPS OIFR APD shall have the meaning given to them in the Policy Document unless otherwise defined in this MPS OIFR APD.

1 Executive summary

1.1 Part 3 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement (LE) purposes.

1.2 Sensitive processing is defined in Part 3 section 35(8). This includes a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; c) the processing of data concerning health; d) the processing of data concerning an individual's sex life or sexual orientation.

1.3 OIFR constitutes sensitive processing primarily because it processes biometric data for the purpose of uniquely identifying individuals. Images processed through OIFR may also incidentally reveal other categories of sensitive personal data, although such characteristics are not actively sought or analysed.

1.4 LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. Given Operator Initiated Facial Recognition (OIFR) involves the processing of biometric data, section 35(3), read with section 35(5), further requires that (a) the processing is strictly necessary for the law enforcement purpose, (b) the processing meets at least one of the conditions in Schedule 8, and (c) at the time when the processing is carried out, the controller has an appropriate policy document in place The MPS OIFR Documents explain the MPS ensures that processing in the course of the MPS's use of OIFR meets the first two of those requirements.

1.5 This document, together with the wider MPS OIFR Documents, demonstrate the MPS's compliance with the third requirement, and demonstrate that the MPS's processing of sensitive data in respect of OIFR is compliant with the requirements with Part 3, Section 42 of the DPA 2018. In compliance with Section 42(2) of the DPA 2018 it explains the procedures and measures for securing compliance with the LE data protection principles and explains the policies as regards retention and erasure of personal data. This document should be treated as being complimentary to the MPS general record of processing under S61 DPA 2018 and the MPS OIFR Documents. It also complements the MPS' policy on protecting special category and criminal convictions policy.

2 Description of Data Processing

THE DATA PROCESSING OPERATIONS RELATED TO OIFR

2.1 The MPS OIFR system is a facial recognition capability which enables a Probe Image of a Permitted Probe Subject to be compared against images contained within a Permitted Image Reference Library. The system returns Potential Matches to the OIFR User for review and Adjudication to determine whether a Viable Match has been identified. Regardless of the means by which the Probe Image is obtained, the core technical operation of OIFR is summarised at Section 3 of the Policy.

2.2 It is clear from the technical operation of OIFR that personal data is processed in relation to two classes of individuals, namely (1) those depicted for searching in a Probe Image and (2) those who feature in an Image Reference Library.

Personal data that is processed when undertaking an OIFR Search

Permitted Image Reference Library Subjects – The following data may be processed to enable operation of the OIFR system and comparison against a Probe Image:	**Permitted Probe Subjects -** The following data may be processed in relation to a Permitted Probe Subject for the purpose of conducting an OIFR Search:

• Subject name
• Facial image, and from/associated with that facial image:
  ○ Biometric facial image template
  ○ Recorded (or if unknown, perceived) gender
  ○ Recorded (or if unknown, perceived) age/date of birth
  ○ Recorded (or if unknown, perceived) ethnicity
  ○ Recorded (or if unknown, any perceived) points concerning a relevant disability/gender transition
  ○ To the extent arising from looking at the image, any perceived religious or philosophical beliefs, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).
  ○ Availability of other biometric modalities (DNA, fingerprints)
  ○ Image meta data (including the time and location where the image was taken).
• Criminal offence data or information concerning why that person is on an Image Reference Library
• Contact details
• Warning markers (e.g. known to possess weapons)
• Note: Further personal data would be available to, and recorded by officers as part of any subsequent investigatory process. This is not data processed by way of OIFR itself, and is instead relevant to the conduct of officers in the normal course of their duties.
	• Probe Image of the subject
	• Information recorded within the OIFR Submission Form relating to the conduct of the OIFR Search.
	• Available to the MPS via the Probe Image
	  ○ Biometric facial image template
	  ○ Perceived gender
	  ○ Perceived age
	  ○ Perceived height
	  ○ Metadata (i.e. location, date and time the footage was captured)/
	  ○ Perceived ethnicity
	  ○ Any perceived points concerning a relevant disability/gender transition
	  ○ On some occasions any perceived religious or philosophical beliefs, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).
	  ○ Image meta data (including the time and location where the image was taken).
	  ○ Details as to the context of the image, for example if the subject is shown as being present with other people.
	• Criminal offence data or other information concerning why that person being submitted as a Probe Image for OIFR Searching.
	• The status of any result – if it is a Potential Match or determined to be a Viable Match.

2.3 In respect of those included within a Permitted Image Reference Library, the Policy identifies the Permitted Image Reference Libraries approved for use (at Section 6) and the process by which additional image libraries may be authorised in accordance with the Policy. Given that these data subjects are already known to the MPS and the Policy does not provide a basis to proactively acquire images solely for inclusion within a Permitted Image Reference Library, much of the underlying data is already processed by the MPS. The process of preparing a Permitted Image Reference Library for OIFR use creates additional data in the form of: (i) a biometric facial image template to enable operation of the OIFR system; and (ii) records demonstrating that an individual has been included within a Permitted Image Reference Library, subject to the retention and deletion provisions set out in the Policy and associated MPS OIFR Documents.

2.4 The form of processing is set out in Section 3 of the Policy and below:

Stage	Action
1	**Permitted Image Reference Library Enrolment**

	A Permitted Image Reference Library is 'enrolled' into the OIFR System. 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**
	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[1] (including the similarity score) will be presented to authorised OIFR Users as further described at paragraph 8.8 and 8.9 of the 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 the Policy.

Personal data processed post-an OIFR Search

2.5 The Policy provides for the completion of an OIFR Submission Form and, where a Potential Match is subsequently determined to be a Viable Match following Adjudication, the creation of a Match Report. Records relating to the conduct and outcome of OIFR Searches are maintained in accordance with the Policy. The retention and deletion of personal data are governed by Section 10 of the MPS

[1] Applicable to the use of OIFR on a hand-held device.

OIFR Policy. In particular:

- Where an OIFR Search does not result in a Viable Match, and no further OIFR Searching is required, the Probe Image and associated OIFR Search data will be deleted in accordance with the retention periods specified in the Policy.
- Where an OIFR Search generates a Potential Match which is subsequently determined to be a Viable Match, OIFR-generated personal data will be deleted as soon as practicable and in accordance with the retention periods specified in the Policy, except to the extent that retention is required: (i) in accordance with the Data Protection Act 2018, Management of Police Information (MoPI), and the Criminal Procedure and Investigations Act 1996; or (ii) in accordance with the MPS complaints, misconduct or conduct investigation processes.
- Permitted Image Reference Libraries are retained and reviewed in accordance with Section 10 of the Policy and the retention requirements applicable to the underlying source data.
- OIFR Submission Forms, Match Reports, audit records and associated governance documentation are retained in accordance with Section 10 of the Policy.

FREQUENCY OF DATA BEING PROCESSED

2.6 Data is processed in relation to specific OIFR Searches conducted on MPS IT systems and devices. The frequency of OIFR Searches is determined by operational demand and the circumstances in which the permitted OIFR use cases set out in the Policy arise.

ALGORITHM ACCURACY

2.7 A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependent on demographic factors. As a result the MPS has had regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST), who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC (the provider used by the MPS). The National Physical Laboratory (NPL) has also undertaken specific operational testing of the MPS OIFR system. The MPS has published a paper entitled 'The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences'. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its OIFR algorithm, including undertaking a process of peer review.

2.8 Results for OIFR showed the best possible performance. For every probe submitted, the correct match was returned at Rank 1 (this is the top match) resulting in a TPIR of 100%. This TPIR is identical for all demographic subgroups and these results show that performance is the same, regardless of race, gender or age.

DATA MANAGEMENT

2.9 See Section 11 of the Policy.

2.10 To ensure the continued accuracy, reliability and proportionality of the OIFR system, the MPS undertakes ongoing system testing and performance benchmarking. Comparative testing is carried out in a fully sandboxed environment with no connectivity to operational systems, production networks or external infrastructure. This programme includes periodic evaluation of algorithm performance, operational validation exercises, and routine monitoring of similarity-score outputs to confirm that the system is operating within expected tolerances and aligned with current and

emerging technological standards.

2.11 Where Potential Matches are later assessed as not viable, the system's continuous assurance process supports early identification of any underlying performance issues. Any discrepancies are examined to determine whether they result from image quality, demographic factors, environmental variables or technical issues, so that appropriate remedial steps can be taken where required. These measures form part of the MPS's data-protection-by-design approach, support the commitment to maintaining optimum system performance, and operate within the retention, review and disposal (RRD) framework established by the OIFR Policy.

DATA SHARING

2.12 Where an OIFR Search results in a Viable Match, subsequent enquiries may involve MPS personnel accessing policing databases, intelligence systems and other information sources in order to inform any further action. Such action may also involve the MPS working with other police forces, law enforcement bodies and partner agencies in the exercise of its policing, safeguarding and national security functions. Whilst this will not ordinarily require the sharing of biometric data generated through the OIFR process, it may require the sharing of personal data, as would occur in the course of any investigation or operational activity, in accordance with applicable legal requirements and the MPS's established information sharing arrangements. The process following an OIFR Search, and any subsequent decision to share data, is no different in principle from that which would arise where an individual had been identified through other lawful means.

3 Consent or Schedule 8 Grounds for Processing

3.1 The MPS OIFR Legal Mandate outlines the legal framework applicable to the use of OIFR. Data will processed under Part III DPA 2018. In reaching this conclusion the MPS has considered (i) the legal position and legislative context (ii) the use cases for OIFR and how they fit in a law enforcement context and (iii) the rights and freedoms of data subjects, including any impact on such subjects from processing data under Part III DPA 2018 as opposed to UK GDPR – notably the right to objective to processing.

3.2 To process data under Part III DPA 2018, the processing needs to fall within a law enforcement purpose. This term is defined at Section 31 and means:

> *'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'*

3.3 The use cases (at Section 2 of the Policy) ensure that the MPS is acting with a law enforcement purpose when it uses OIFR.

3.4 OIFR also involves the processing of biometric data for the purpose of uniquely identifying individuals and therefore constitutes sensitive processing for the purposes of section 35(3) DPA 2018. In order to undertake such processing, the MPS must satisfy the requirements of section 35 DPA 2018. The processing must be strictly necessary for the relevant law enforcement purpose, satisfy a condition set out in Schedule 8 DPA 2018, and be undertaken in accordance with an appropriate policy document.

3.5 The MPS considers that Schedule 8, paragraph 1 applies to the use of OIFR. This condition is met where the processing is necessary for the exercise of a function conferred by an enactment or rule

of law and is necessary for reasons of substantial public interest. The specific policing purpose, necessity case and justification for undertaking an OIFR Search are recorded through the OIFR Submission Form process.

Consent and the acquisition of Probe Images

3.6 **Acquisition of Probe Images**: Under Use Case A, a Probe Image may be acquired either through the individual's real and informed consent or pursuant to using common law powers. Where reliance is placed upon consent, officers should ensure that the individual is informed, in clear terms, of the purpose for which the image is being obtained, including that it may be used to undertake an OIFR search.

3.7 **OIFR Searches** The basis for processing data as an OIFR search is distinct from the legal basis on which a Probe Image is acquired.

3.8 OIFR may only be used where it is for a law enforcement purpose, is strictly necessary in the particular circumstances of the case, and is proportionate to the legitimate aim pursued. As biometric data is processed for the purpose of uniquely identifying an individual, the processing must also satisfy the requirements for sensitive processing under section 35 of the Data Protection Act 2018.

3.9 Accordingly, the fact that an individual has consented to the acquisition of a Probe Image does not, of itself, justify the use of OIFR. Officers must independently satisfy themselves that the requirements of this Policy are met and that any OIFR search is lawful, strictly necessary and proportionate in all the circumstances.

4 Procedures for ensuring compliance with the principles

PRINCIPLE (1) LAWFUL AND FAIR

4.1 Under s.35(2), the processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law. The MPS OIFR Legal Mandate sets out the legal framework governing the use of OIFR and the statutory and common law functions that OIFR supports.

4.2 Under s.35(2), such processing is lawful only to the extent that (a) the data subject has given consent to the processing for that purpose, or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority. In addition, because the use of OIFR involves the deployment of sensitive personal data (and the MPS does not rely on consent), the processing must be strictly necessary for the law enforcement purpose under s.35(5)(a). Finally, because the MPS relies on the first paragraph of Schedule 8 in order to meet the requirement in s.35(5)(b), it must be the case that such processing: (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest.

4.3 The Policy incorporates a number of safeguards designed to ensure that OIFR is used only where the processing is lawful, strictly necessary and proportionate. In particular, the Policy:

- restricts the use of OIFR to defined and approved use cases;
- limits the categories of individuals who may be submitted as Permitted Probe Subjects;
- restricts searching to approved Permitted Image Reference Libraries;
- requires completion of an OIFR Submission Form;
- requires decision makers to consider whether less intrusive measures are available and whether the proposed search is necessary and proportionate in all the circumstances; and

- requires that the specific policing purpose for the search is recorded and capable of subsequent audit.

4.4 The Policy further governs the acquisition of Probe Images (Section 4) and restricts the categories of individuals who may be treated as Permitted Probe Subjects (Section 5), ensuring that OIFR Searches are undertaken only where the circumstances fall within an approved use case and there is a legitimate policing need as set out in the Policy. Likewise, the Policy restricts the Image Reference Libraries against which OIFR Searches may be undertaken (Section 6).

4.5 Although the lawfulness of processing in respect of any particular OIFR Search will depend on the circumstances of that Search, the substantial public interests served by the use of OIFR including the detection and investigation of criminal offences, the protection of life, and the advancement of policing investigations in line with the OIFR Use Cases.

4.6 The MPS is also subject to obligations under the Human Rights Act 1998. Compliance with the Policy, and in particular with Section 7 (Proportionality), serves to ensure that Deployments are undertaken only in compliance with the 1998 Act.

4.7 The MPS is also subject to obligations under the Equality Act 2010. The MPS has considered the equality impacts of OIFR in general by way of its Equality Impact Assessment, and continues to keep these under review by way of regular review by the FRT Board. In accordance with the Policy, OIFR Users consider equality considerations as part of the completion of the OIFR Submission Form.

4.8 Compliance with the OIFR Policy will also ensure that sensitive processing is fair. Fairness is embedded both in the design of the Policy and in the assessment process required through completion of the OIFR Submission Form, which obliges decision makers to demonstrate that each proposed OIFR Search is necessary, proportionate and responsive to a permitted OIFR use case. The Policy—including in particular Section 7 on proportionality—requires focused and structured consideration of the impact of processing on affected individuals, including explicit evaluation of Article 8 ECHR privacy expectations, the sensitivity of imagery (by reference to the Image Matrix), protected characteristics (Annex D), and the steps available to minimise intrusion. This ensures that OIFR Searches are undertaken only where the likely impact on the rights and freedoms of individuals has been identified, assessed and justified. The assessment process further requires decision makers to consider the reasonable expectations of privacy of persons whose images are processed and whether the proposed OIFR Search strikes a fair balance between the rights of those individuals and the legitimate policing objective being pursued. In addition, the MPS OIFR Documents, including the OIFR Policy, DPIA, EIA, APD and Privacy Notice, are published to support transparency and public understanding of how OIFR is used. These measures help ensure that OIFR processing remains fair, transparent and accountable.

PRINCIPLE (2) PURPOSE LIMITATION

4.9 Section 2 of the OIFR Policy sets out the only permissible use cases for the MPS's use of OIFR. OIFR Searches may be conducted only for one of those approved use cases and for the specific policing purpose recorded within the OIFR Submission Form. If, during the course of an investigation or operation, the policing purpose changes such that it no longer aligns with the original use case or justification, a new OIFR Submission Form must be completed and the revised use independently assessed for legality, necessity and proportionality before any further OIFR Search is undertaken.

4.10 The DPIA provides an assessment of the risk to the rights and freedoms of data subjects in relation to Principle 2 and identifies the mitigations which apply. Amongst other safeguards, the Policy and Annexes govern the lawful acquisition and use of Probe Images and limit the circumstances in which

imagery may be used for OIFR. Probe Images must be obtained and processed only for a legitimate policing purpose falling within an approved OIFR use case.

4.11 The Policy also limits the circumstances in which Image Reference Libraries may be used and requires that OIFR Searches are undertaken only against approved Permitted Image Reference Libraries relevant to the policing purpose being pursued. These controls help ensure that personal data is processed only for the specific law enforcement purpose that justified the search.

4.12 Furthermore, compliance with Section 11 of the OIFR Policy (Data Management) ensures that sensitive data generated during OIFR use is not processed in a manner incompatible with the purpose for which it was collected. Section 11 sets out clear requirements for the retention and deletion of biometric templates.

PRINCIPLE (3) DATA MINIMISATION

4.13 The OIFR Policy sets out the only permissible OIFR use cases (Section 2), and OIFR may only be used where it is necessary for one of those defined policing purposes. Data minimisation is supported through a number of policy controls, including:

- the requirement that Probe Images are obtained and used only in accordance with the permitted use cases and requirements set out in the Policy;
- direction on the acquisition of Probe Images (Section 4) and restrictions on the categories of individuals who may constitute Permitted Probe Subjects (Section 5);
- restrictions on the Image Reference Libraries against which OIFR Searches may be conducted (Section 6);
- the requirement to complete an OIFR Submission Form demonstrating the necessity and proportionality of the proposed search;
- the requirement to consider whether less intrusive measures are available and capable of achieving the relevant policing objective; and
- requirements governing the review, retention and deletion of OIFR data.

4.14 Compliance with the OIFR policy requirements ensures that OIFR processing is limited to the minimum amount of data necessary to achieve legitimate policing objectives.

4.15 Section 11 of the Policy (Data Management) also supports data minimisation by setting strict requirements for the review, retention and deletion of imagery, biometric templates and Image Reference Library material.

PRINCIPLE (4) ACCURACY

4.16 The MPS OIFR DPIA provides an assessment of the risks to the rights and freedoms of data subjects in relation to Principle 4 (Accuracy) and identifies the mitigations that apply. The Policy and supporting OIFR governance documents incorporate a number of technical, procedural and operational safeguards designed to ensure that personal data processed through OIFR is accurate, relevant and up to date. These include:

- Image quality and suitability controls: Annex C sets out the requirements applicable to Probe Images and Image Reference Libraries. OIFR Users must ensure that images are suitable for facial comparison purposes and represent the most appropriate image available for the relevant policing purpose.
- Controls on the source, relevance and currency of imagery: Probe Images and Image Reference Library images must be lawfully obtained, relevant to the approved use case and processed in accordance with the requirements of the Policy. Image Reference Libraries are subject to review and retention controls to ensure continued necessity and

relevance.

- Training and guidance for OIFR Users: OIFR Users receive training on the operation of the system, the adjudication process, and the factors which may affect match reliability, including image quality, time lapse, and Subject, System and Environmental factors. This assists users in making informed and consistent adjudication decisions.
- Automated quality controls: The OIFR System includes automated quality checks designed to identify poor-quality or otherwise unsuitable images before biometric comparison takes place, reducing the risk of inaccurate results arising from unsuitable imagery.
- Similarity score threshold: The OIFR System applies a similarity score threshold designed to reduce the presentation of low-confidence results for adjudication. The threshold forms part of the MPS's data protection by design approach and assists in improving the accuracy and reliability of OIFR outcomes.
- Human adjudication: OIFR does not treat a Potential Match as definitive. Every Potential Match is subject to adjudication by a trained OIFR User who must consider image quality, facial similarity, the age and context of the images, and any other relevant factors when determining whether a Potential Match constitutes a Viable Match. A Potential Match is not confirmation of identity.
- Accuracy of associated information: Where a Viable Match is identified, any information subsequently accessed by officers remains subject to existing MPS data quality, review and correction processes. This assists in reducing the risk of operational decisions being based on inaccurate or out-of-date information.
- Algorithm performance and demographic considerations: The MPS has regard to independent testing, operational performance data and demographic accuracy assessments when evaluating the OIFR system. The MPS also undertakes ongoing testing and performance benchmarking to monitor system performance and identify any issues affecting accuracy or reliability.
- Data management controls: Section 11 of the Policy (Data Management) establishes requirements governing the review, retention and deletion of OIFR data to ensure that inaccurate, out-of-date or unnecessary information is not retained within the system.

4.17 Collectively, the measures set out in the OIFR Documents ensure that the personal data processed by the OIFR System is sufficiently accurate, reliable and current for the policing purposes for which it is used, and that the system's outputs remain subject to robust human review and safeguards.

Inaccuracies in the algorithm

4.18 The MPS OIFR DPIA provides an assessment of the risks to the rights and freedoms of data subjects relating to potential inaccuracies in the OIFR algorithm and identifies the mitigations that apply. Among other points:

- Algorithm Performance and ICO Guidance: The ICO guidance confirms that compliance with the accuracy principle does not require 100% statistical accuracy but does require robust measures to ensure reliability, fairness, and proportionality. The MPS applies these standards to OIFR embedding accuracy and equality considerations into governance and operational practice.
- Algorithm performance and independent testing: The performance of the facial recognition algorithm used by OIFR has been independently evaluated by the National Physical Laboratory (NPL) and subjected to external scrutiny. In its 2023 Equitability Study, NPL found that, for the OIFR use case evaluated, the correct reference identifier was returned at Rank 1 for every probe image submitted, representing a True Positive Identification Rate (TPIR) of 100%. NPL further found that this performance was consistent across the demographic groups tested and did not identify demographic

performance variation. These findings provide assurance regarding the accuracy, reliability and fairness of the algorithm under operationally representative conditions.

- Similarity score threshold: The OIFR System is configured with a similarity score threshold designed to reduce the impact of poor-quality imagery and minimise the return of unsuitable results for Adjudication. The threshold has been informed by independent testing undertaken by the National Physical Laboratory (NPL), including findings that, excluding identical twins, non-mated comparison scores fell below the threshold selected by the MPS, whilst genuine matches continued to be returned save in a small number of cases involving image quality issues. The threshold is presently set at 6600 (0.66) and forms part of the MPS's data protection by design approach. By reducing the presentation of low-confidence results for Adjudication, the threshold assists in improving the accuracy and reliability of OIFR outcomes. The threshold will remain subject to review by the Senior Responsible Owner (SRO), who may authorise adjustments where supported by operational experience, performance monitoring, technical assurance, audit findings or further testing, in order to ensure that the OIFR System remains accurate, effective and proportionate.
- Algorithm assurance and governance: The OIFR System operates under approved and tested configurations. Any material amendment to the algorithm, threshold settings or technical operation of the system would require governance consideration, including through the FR Technology Board and, where necessary, further impact assessment.
- Human-in-the-loop Adjudication and Match Report controls: Potential Matches are reviewed by trained OIFR Users before being deemed Viable Matches. OIFR Users must consider image quality, Subject, System and Environmental factors together with factors supporting or undermining confidence in the match. Results which do not justify further action must not be treated as Viable Matches.
- Equality monitoring: The FR Technology Board reviews information relating to system performance, demographic outcomes and equality impacts. This assists in identifying emerging trends and enables operational, governance or technical changes to be considered where appropriate.
- Training and guidance for OIFR Users: OIFR Users receive training on system capabilities and limitations, image quality, Adjudication, equality considerations and factors affecting match reliability. This reduces the risk of inappropriate reliance being placed on algorithmic outputs.

4.19 Collectively, these measures ensure that any residual inaccuracies or performance limitations of the OIFR algorithm are identified, mitigated and continuously monitored, and that the system's outputs are not treated as determinative.

PRINCIPLE (5) RETENTION

4.20 Data is processed in accordance with Part 3 DPA 2013 and subject to Section 11 (Data Management) of the Policy which sets out applicable retention periods.

4.21 The MPS maintains records of processing activities in compliance with Section 61 DPA 2018, and complies with Section 62 DPA 2018 in relation to the operation of the OIFR System.

PRINCIPLE (6) SECURITY

4.22 Security of personal data processed by the OIFR System is ensured through the combined requirements of the OIFR Policy, the OIFR DPIA and wider MPS information-security standards. Collectively, these measures ensure the integrity, confidentiality and availability of personal data

processed by the OIFR System, in accordance with Principle 6.

5 Policy applicable to retention and erasure

5.1 Section 11.1 of the Policy provides that:

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:*

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 0 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.

6 Protective Marking

Classification	Official
Suitable for Publication	Yes
Title	APD relating to the use of Operator Initiated Facial Recognition by the MPS.
Purpose	To explain the procedures and measures for securing compliance with the LE data protection principles and explains the policies as regards retention and erasure of personal data.
Author	MPS OIFR
Version	1.0
Creating Unit	MPS OIFR
Date Created	1 November 2026
Review Date	1 November 2027