

More Trust | Less Crime | High Standards

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

1 Executive summary _____ 3

2 The Purpose, Benefits and Attitudes to RFR _____ 5

3 Description of Data Processing_____ 7

4 The Principal Impacts of RFR _____ 13

5 Data Protection and 'Privacy Law' Assessment_____ 19

6 Individual Rights _____ 41

7 Conclusion _____ 45

8 Data Protection Impact Assessment Sign-off_____ 45

9 Protective Marking _____ 48

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

1 Executive summary

1.1 As a `public body', the Metropolitan Police Service (MPS) is subject to the requirements and conditions imposed by the Human Rights Act 1998, the Equality Act (EA) 2010 and the Data Protection Act (DPA) 2018. These include an obligation on the MPS to process personal data fairly and lawfully in order to safeguard the rights and freedoms of individuals.

1.2 Section 64 of the DPA 2018 mandates the completion of a Data Protection Impact Assessment (DPIA) for organisations processing data under Part III where this processing is likely to result in a high risk to the rights and freedoms of data subjects.

1.3 This DPIA outlines the processing operations involved in the Deployment of Operator Initiated Facial Recognition (OIFR) and how they serve the public interest in effective law enforcement.

1.4 OIFR differs from other facial recognition capabilities currently used by policing. Unlike Live Facial Recognition (LFR), OIFR does not involve the biometric processing of all persons passing through a Zone of Recognition. Unlike Retrospective Facial Recognition (RFR), OIFR involves the acquisition or capture of an image of a subject and the comparison of that image against an approved facial image gallery for a specific operational purpose, rather than the analysis of an image already lawfully held by policing. As a result, the privacy impacts considered by this DPIA arise both from the acquisition of the image itself and from the subsequent biometric comparison process.

1.5 This DPIA recognises that data processed as a result of using the MPS's OIFR system will occur under Part III DPA and involves (i) innovative technology, (ii) biometric data resulting in sensitive processing for the purposes of Section 35(3) DPA, (iii) data relating to criminal convictions and offences, (iv) data matching and (v) the possible consequences of a match outcome, including the generation of intelligence leads, support for further investigatory activity, and information capable of informing arrest, detention, law enforcement-led safeguarding and risk-management decisions. Absent appropriate safeguards, the MPS's use of OIFR would pose high risks to affected data subjects. This DPIA outlines the extensive safeguards put in place by the MPS, and the MPS's assessment that these are sufficient to secure that (i) the processing is not high risk, and (ii) in all the circumstances the processing is necessary and proportionate to achieve the MPS's legitimate aim of enhancing its ability to achieve its policing purposes.

USE OF THE MPS OIFR DPIA

1.6 Advice issued by the Information Commissioner's Office (ICO) is that the DPIA process should commence during the very early stages of a project and most certainly before any data is processed. Work on the DPIA should run alongside the planning and development process. The DPIA should remain a living document, subject to review as the project develops to ensure currency and that the risks and mitigations remain accurate and effective.

1.7 This document is designed to be used as an overarching DPIA to support using the MPS's OIFR system. The OIFR Submission Form requires further search-specific impact assessment points to be considered relating to the rights and freedoms of data subjects, and together with this overarching DPIA, forms an integral part of the DPIA applicable to a given OIFR Search.

1.8 This document should be read in conjunction with the MPS OIFR Documents, including in particular the OIFR Policy (the "Policy"), which restricts the circumstances in which OIFR may be used and puts in place several safeguards in relation to its use.

ROLE OF THE DATA PROTECTION OFFICER

1.9 Policy development: The Data Protection Officer (DPO) is available to provide advice and input to process by which OIFR policy is developed and the technology used. The roles of the DPO and the Data Office are an important part of the process when considering an OIFR Search and advice from a data protection perspective would assist. As well as providing advice, the DPO is able to monitor compliance with the DPA 2018, and in doing so provides assurance to the MPS Commissioner. Both this overarching DPIA and records relating to particular cases provide a means to capture a record of any advice or input received from the DPO.

1.10 **Colleagues are encouraged to make early contact with the Data Office mailbox regarding the use of OIFR.**

1.11 Ongoing Review: The DPO and Data Office's role continues throughout the use of, and after OIFR Searching. They act as points of contact and provide ongoing assurance in relation to data processing queries. They also facilitate data subjects' exercise of their individual rights and support instances where trends or concerns are identified via their attendance at the MPS FR Technology Board.

1.12 Within the MPS the senior internal oversight body for OIFR is the MPS FR Technology Board, which in turn answers to the MPS Management Board. The DPO sits on the MPS FR Technology Board and as such is able to retain oversight on the conduct of MPS OIFR use.

2 The Purpose, Benefits and Attitudes to OIFR

BENEFITS OF OIFR

2.1 OIFR can assist officers and investigators by enabling the comparison of a Probe Image of a Permitted Probe Subject against relevant Permitted Image Reference Libraries in real or near-real time. This capability supports the development of intelligence where a subject's identity is unknown or in doubt and can inform policing decisions in live and dynamic operational contexts.

2.2 OIFR involves both the acquisition of a Probe Image and its subsequent biometric comparison against a Permitted Image Reference Library. The MPS recognises that each stage engages privacy rights. However, in appropriate circumstances OIFR may represent a less intrusive means of progressing identity-related enquiries than alternatives such as arrest, prolonged detention, physical biometric capture, or extensive manual enquiries. The necessity and proportionality of each OIFR Search is therefore assessed by reference to the particular circumstances of the case and the safeguards contained within the Policy and associated MPS OIFR Documents.

2.3 OIFR can support officers and investigators to:

- develop intelligence leads where identification would otherwise remain unresolved or would require more resource-intensive or intrusive interventions. In some cases, this may enable matters to be resolved at the point of encounter without the need for arrest or detention, while supporting more informed risk management and progression of investigations and operations;
- support identification in circumstances where other methods (such as fingerprints or biographical checks) are unavailable, inconclusive, or would not return a result, by making use of facial imagery held within Permitted Image Reference Libraries;
- support timely operational decision-making in fast-moving or uncertain policing environments;
- support less intrusive policing outcomes, including reducing the need for arrest, detention, or physical biometric capture (e.g. fingerprints or DNA) where identity can be sufficiently progressed through OIFR; and
- reduce reliance on manual or resource-intensive enquiries which may delay the progression of an investigation or operational activity.

2.4 In this way, OIFR supports operational effectiveness without removing the requirement for human judgement, further lawful investigation, or corroboration. Any Potential Match generated by the OIFR System must be subject to Adjudication and, even where assessed to be a Viable Match, remains an intelligence lead rather than definitive evidence of identity.

OPERATIONAL VALUE

2.5 OIFR is particularly valuable in circumstances where the timely establishment of identity or effective management of risk is necessary to support policing objectives. This reflects the defined permitted use cases for OIFR, namely:

- identifying an unknown subject to advance a policing investigation or operation; and
- ascertaining whether an arrested or otherwise detained person poses a risk to themselves or others.

2.6 In these contexts, OIFR may assist to:
- progress investigations or operational activity where identity is a relevant factor;
- support safeguarding, including where an individual may present a risk to themselves or others, enabling investigations to progress efficiently and effectively; and
- enable more informed and proportionate responses in fast-moving or uncertain circumstances.

2.7 Operationally, OIFR may assist both:
- at the point of encounter, where an officer is required to make real-time decisions; and
- within controlled environments, including custody or police premises, where timely access to identity-linked information supports the safe and lawful management of individuals.

OPERATIONAL IMPACT

2.8 The use of OIFR has the potential to enhance policing efficiency and effectiveness by:
- enabling earlier identification and better risk management where alternative methods would be insufficient, more impactful or too slow in the circumstances; and
- reducing delay in progressing investigations or making operational decisions.

2.9 By supporting earlier and more informed decision-making, OIFR can contribute to a more effective use of policing resources and improved management of risk, while remaining subject to the safeguards, proportionality requirements, and oversight mechanisms set out in this Policy and associated MPS OIFR Documents.

ILLUSTRATIVE OPERATIONAL EXAMPLES

2.10 **Identification of an unknown subject:**

An officer encounters a subject whose identity is unknown and relevant to an investigation. A Probe Image is lawfully captured and searched using OIFR, generating a Potential Match which, following Adjudication, assists in developing an intelligence lead. This enables further proportionate enquiries to be undertaken without delay, supporting progression of the investigation.

2.11 **Custody and risk management:**

In a custody or other detention setting, OIFR may be used where it is necessary to establish whether information held by the MPS is relevant to a detained individual. This

may be particularly important where a person provides false details, uses an alias, or where their identity cannot otherwise be reliably established. For example, a search may identify information indicating risks relating to violence, self-harm, vulnerability, safeguarding concerns, or that the individual is wanted in connection with a more serious offence. This supports more informed decision making in relation to detention, welfare and safeguarding, particularly where biographical checks alone would not be viable or sufficiently reliable in the circumstances. By enabling relevant information to be identified at an earlier stage, OIFR would also support the safe, efficient and effective operation of custody and detention environments.

PUBLIC ATTITUDES TO FACIAL RECOGNITION AND OIFR

2.12 Public trust and legitimacy are central considerations in the MPS's use of facial recognition technologies, including OIFR. The Mayor's Office for Policing and Crime (MOPAC) Public Attitude Survey continues to assess Londoners' views regarding policing technologies and facial recognition. Recent survey findings indicate that a substantial majority of Londoners support the use of innovative technologies by the police where their use is subject to appropriate safeguards, oversight and accountability arrangements

2.13 The MPS has undertaken engagement with communities, representative groups and stakeholders regarding the use of facial recognition technologies. Whilst views differ as to the circumstances in which facial recognition should be used, public feedback has generally identified greater acceptance of targeted uses of facial recognition than technologies involving pervasive population scanning. OIFR has been designed as a targeted capability, restricted to defined use cases and subject to legal, operational and governance safeguards, including individual necessity and proportionality assessments, audit requirements and oversight arrangements.

CONSULTATION

2.14 A record of consultation is maintained in the MPS OIFR EIA.

3 Description of Data Processing

THE DATA PROCESSING OPERATIONS RELATED TO OIFR

3.1 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.

3.2 OIFR involves the acquisition or capture of an image of an individual for the purpose of conducting a facial recognition search. Accordingly, personal data is processed in relation to two broad categories of individual: (1) the Permitted Probe Subject whose

image is acquired and searched, and (2) those individuals whose images are held within a Permitted Image Reference Library and against whom the comparison is undertaken.

3.3 The processing of personal data through OIFR occurs at several stages, including acquisition of the Probe Image, extraction of biometric facial data, comparison against a Permitted Image Reference Library, Adjudication of any Potential Match, and recording of the search outcome. This DPIA considers the privacy impacts arising from each stage of that processing.

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.

3.4 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.

3.5 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 **Error! Reference source not found.** and **Error! Reference source not found.** 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

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

	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 **Error! Reference source not found.** of this Policy.

Personal data processed post-an OIFR Search

3.6 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 11 of the MPS 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 11 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 11 of the Policy.

FREQUENCY OF DATA BEING PROCESSED

3.7 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.

FACTORS AFFECTING THE RISK OF OIFR PROCESSING

3.8 Absent appropriate safeguards, the processing embodied by the MPS's use of OIFR would be likely to result in a high risk to the rights and freedoms of individuals. Factors affecting that assessment of risk are as follows.

3.9 **Innovative Technology**: OIFR makes use of facial recognition technology to compare a Probe Image against images contained within a Permitted Image Reference Library. Whilst facial recognition technology has been used by policing for a number of years, it

continues to develop in capability and functionality. OIFR has been used by other UK Police Forces, notably South Wales Police, but this is a new capability to the MPS. Appropriate governance, technical assurance, training and oversight are therefore required to ensure that its use remains lawful, necessary and proportionate.

3.10 **Acquisition of Imagery for Biometric Processing**: OIFR involves the acquisition or capture of an image of an individual for the purpose of conducting a facial recognition search. The acquisition of a Probe Image may itself engage privacy rights and, absent appropriate safeguards, may represent a significant intrusion into an individual's private life. The Policy therefore restricts the circumstances in which OIFR may be used and requires consideration of the necessity and proportionality of each OIFR Search.

3.11 **Biometric Data**: The OIFR system processes biometric data, both in relation to those included within a Permitted Image Reference Library and those depicted in a Probe Image. By its nature, this is high risk and means the MPS is undertaking sensitive processing for the purposes of section 35(3) DPA 2018. Security measures, including safeguards by design, have been identified and implemented in this DPIA and the MPS OIFR Documents to mitigate risks associated with biometric data processing.

3.12 **Criminal offence data**: The use of the OIFR system may involve the processing of criminal offence data and other policing information in relation to individuals included within Permitted Image Reference Libraries. Whilst this may involve comparatively large-scale processing at the point the libraries are maintained, the OIFR User is only presented with Potential Match(es) returned by the system and information subsequently reviewed following a Viable Match.

3.13 **Data Matching**: OIFR works by analysing facial features within a Probe Image to generate a biometric facial template. This template is then compared against biometric templates derived from images contained within a Permitted Image Reference Library in order to identify Potential Matches. The Adjudication process requires human review and decision-making, and additional mitigations have been identified and implemented in this DPIA and the MPS OIFR Documents.

3.14 **Possible results of a match:** An OIFR Potential Match may, following Adjudication, lead to a Viable Match being determined and used as an intelligence lead for further operational activity. This may support further enquiries, safeguarding activity, detention-related decision making, risk management measures, investigative action or, where lawful grounds otherwise exist, arrest. OIFR does not itself establish identity and neither a Potential Match nor a Viable Match, without more, justifies enforcement action. The processing embodied by OIFR may nevertheless contribute to a sequence of events that affects an individual's rights and freedoms and therefore requires robust safeguards, oversight and accountability mechanisms.

ALGORITHM ACCURACY

3.15 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.

3.16 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

3.17 See Section 11 of the Policy.

3.18 To ensure the continued accuracy, reliability and proportionality of the OIFR system, the MPS undertakes ongoing system testing and performance benchmarking. This includes periodic evaluation of algorithm performance, operational validation exercises, and routine monitoring of similarity-score outputs to confirm that the system operates within expected tolerances. These measures support early identification of any performance issues and enable investigation of instances where Potential Matches are later assessed as not viable. Discrepancies are analysed to determine whether they arise from image quality, demographic factors, environmental variables or technical issues, so remedial steps can be taken if required. This continuous assurance process forms part of the MPS's data-protection-by-design measures, supports the commitment to maintaining optimum system performance, and operates within the RRD framework established by the OIFR Policy.

DATA SHARING

3.19 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.

4 The Principal Impacts of OIFR

THOSE WHOSE IMAGES ARE PROCESSED AS A PROBE IMAGE VIA AN OIFR SEARCH

4.1 Where an OIFR Search is undertaken, a Probe Image depicting one or more Permitted Probe Subjects is obtained and processed in the manner described in Section 3 of this DPIA. OIFR therefore involves both the acquisition of an image for the purpose of conducting a facial recognition search and the subsequent processing of facial biometric data. Facial biometric data is intrinsically private in nature and unconstrained processing of such data would pose a significant risk to the rights and freedoms of individuals.

4.2 The acquisition of a Probe Image may itself engage privacy rights. Depending on the circumstances, an individual may be photographed in a public place, a private setting, a custody or detention environment, or whilst interacting with police officers in circumstances where identity is relevant to a policing purpose. Absent appropriate safeguards, the acquisition and retention of Probe Images and associated biometric templates could result in the creation of records concerning individuals who have been subject to biometric identification processes irrespective of the outcome of the OIFR Search.

4.3 The biometric comparison process also engages privacy rights. OIFR is intended to support the identification of an individual, or the verification of information concerning that individual, through comparison against a Permitted Image Reference Library. Any Potential Match generated by the OIFR System may influence operational decision making, including decisions relating to investigations, safeguarding, detention, welfare and risk management. Whilst OIFR does not itself establish identity and neither a Potential Match nor a Viable Match, without more, justifies enforcement action, the results of an OIFR Search may contribute to a sequence of events affecting an individual's rights and freedoms.

4.4 The MPS recognises that the use of facial recognition technology has the potential to create a chilling effect on the exercise of fundamental rights. Absent appropriate safeguards, concerns about images being obtained and subjected to biometric processing may affect an individual's willingness to participate in lawful protest and assembly, express views publicly, associate with others, or engage in aspects of their private and family life. The restrictions and safeguards contained within the Policy are intended to minimise these risks and ensure that OIFR is used only where necessary and proportionate for a legitimate policing purpose.

4.5 The MPS's policing objectives for OIFR, and the safeguards built into this Policy, mean that an unconstrained approach is neither required nor possible. OIFR may only be used:

- in a permitted 'Use Case' (as defined in Section 2 of the Policy);
- where the Probe Image has been acquired pursuant to Section 4 of the 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 of the Policy);

- against Permitted Image Reference Libraries (as set out in Section 6 of the Policy);
- in compliance with the rules on Images (as set out in Annex C of the Policy);
- in compliance with the rules on Protected Characteristics (as set out in Annex D of the Policy);
- where its use is proportionate in all the circumstances (in accordance with the guidance in Section 7 of the Policy) and
- subject to the requirements as to transparency set out in Section 12 of the Policy.

4.6 Additionally, the impact on those whose images are processed is further reduced by the following safeguards:

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

- **Controls on image acquisition**: Probe Images may only be obtained in accordance with Section 4 of the Policy and used in accordance with Annexes C and D. The Policy contains additional safeguards where imagery gives rise to elevated privacy expectations, wider human rights considerations, equality considerations, or involves children, disability or gender reassignment

- **Privacy by design ingestion**: Where multiple faces are present in a Probe Image, only the face selected and confirmed by the OIFR User as belonging to a Permitted Probe Subject proceeds to biometric comparison. This limits the processing of biometric data to those individuals who satisfy the requirements of the Policy.

- **Algorithm accuracy and fairness:** The performance of the facial recognition algorithm has been independently evaluated by the National Physical Laboratory (NPL), including in relation to OIFR, and subjected to external scrutiny. Testing demonstrated high levels of accuracy and did not identify demographic performance variation across the groups tested. In addition, all Potential Matches are subject to human review and Adjudication before any determination is made that a Viable Match exists.

- **Similarity score threshold:** The OIFR System is configured with a similarity score threshold designed to minimise the return of irrelevant images and reduce the likelihood of false matches being presented 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. 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.

- **OIFR Submission Form and Image Tier controls**: Every OIFR Search must be supported by a completed OIFR Submission Form, providing a structured mechanism to ensure compliance with the Policy's operational, legal and governance safeguards. The Policy also imposes controls based on the applicable Image Tier, with enhanced safeguards, approvals and scrutiny applying where an image gives rise to elevated privacy, equality or wider human rights considerations.

- **Human-in-the-loop adjudication:** Potential Matches are returned for Adjudication by a trained OIFR User. Any determination that a Potential Match constitutes a Viable Match is subject to human assessment and appropriate recording.

- **Data minimisation and deletion:** Probe Images, biometric templates and associated OIFR records are subject to strict retention and deletion requirements in accordance with Section 11 of the Policy.

- **Audit and governance controls:** OIFR Searches are subject to audit, oversight and governance arrangements, including record keeping through the OIFR Submission Form process and review through established MPS governance structures.

- **Protected characteristics safeguards:** Enhanced approval and handling requirements apply where OIFR is proposed in relation to children, disability, gender reassignment or other protected characteristics, in accordance with Annex D of the Policy.

- **Intelligence status:** The Policy makes clear that a Potential Match or Viable Match constitutes an intelligence lead only and does not, by itself, justify arrest, search, detention or other enforcement action. Any subsequent policing activity must be lawful, necessary and proportionate and capable of independent justification.

- **Transparency measures:** The MPS publishes the OIFR Policy and associated impact assessments and facilitates the exercise of individual rights in accordance with the Data Protection Act 2018. OIFR use is also subject to reporting, oversight and accountability arrangements.

4.7 By design, OIFR is a targeted facial recognition capability which may only be used in defined circumstances and subject to the safeguards described above. Controls exist in relation to the acquisition of Probe Images, the categories of individuals who may be searched, the image libraries that may be used, the conduct of Adjudication, and the retention and deletion of data. The safeguards set out in Sections 4.5 and 4.6 of this DPIA are intended to ensure that the privacy impact arising both from the acquisition of a Probe Image and its subsequent biometric processing is appropriately mitigated and justified in all the circumstances, having regard to the benefits of OIFR and its role in supporting policing, safeguarding and risk-management objectives identified in Section 2 of this DPIA.

THOSE WHOSE IMAGES ARE IN AN OIFR IMAGE REFERENCE LIBRARY

4.8 For individuals whose images are contained within Permitted Image Reference Libraries, their data is processed in the manner described at Section 3 of this DPIA. If facial recognition were unconstrained in terms of which libraries may be used and how, there would be risks of abuse and arbitrariness—including speculative, repeated checks disproportionate to the policing aim where less intrusive options are viable. Such an approach could have a chilling effect on individuals' willingness to go about their daily lives, participate in lawful assemblies, or otherwise exercise their Convention rights. In addition, inclusion within an Image Reference Library means that a person's image may be compared against Probe Images submitted for OIFR Searches, creating a risk that individuals may be identified and linked to policing activity in circumstances where inappropriate library selection, retention or governance controls are not in place.

4.9 The MPS's policing objectives for OIFR, and the safeguards adopted by this Policy, ensure that an unconstrained approach is neither required nor possible. Notably, OIFR is tightly constrained to permit use only:

- in a permitted 'Use Case' (as defined in Section 2 of the Policy);
- where the Probe Image has been acquired pursuant to Section 4 of the 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 of the Policy);
- against Permitted Image Reference Libraries (as set out in Section 6 of the Policy);
- in compliance with the rules on Images (as set out in Annex C of the Policy);
- in compliance with the rules on Protected Characteristics (as set out in Annex D of the Policy);
- where its use is proportionate in all the circumstances (in accordance with the guidance in Section 7 of the Policy) and
- subject to the requirements as to transparency set out in Section 12 of the Policy.

4.10 The risks outlined at 4.8 are further mitigated as follows:

- **Already-held imagery:** Images included within Permitted Image Reference Libraries are already lawfully held by the MPS and subject to their own retention regimes. The principal new data created by OIFR are (i) biometric templates generated to enable facial comparison and (ii) records evidencing that an OIFR Search was conducted and, where applicable, that a Potential Match or Viable Match was identified.

- **Algorithm accuracy and fairness:** The performance of the OIFR algorithm has been independently tested by the National Physical Laboratory (NPL) and peer-reviewed to confirm high statistical accuracy and demographic parity. The NPL found a True Positive Identification Rate of 100% at Rank 1 with no statistically significant differences across race, gender, or age groups.

- **Similarity score threshold:** The OIFR System is configured with a similarity score threshold designed to minimise the return of irrelevant images and reduce the likelihood of false matches being presented 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. 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.

- **Segregation of categories:** The technical design of the OIFR system ensures that different categories of persons (e.g., wanted by the courts, missing persons, victims) are apparent. This prevents inappropriate conflation and ensures investigators understand why an image is included, informing proportionate action.

- **Library governance controls:** Only Permitted Image Reference Libraries authorised under Section 6 of the Policy may be used, reducing the risk of inappropriate or speculative searching.

- **Image Tier and Library Selection Controls**: Annex C applies a structured image classification framework based on privacy, human rights and equality considerations. Suitable compliant police-originated images, which attract the lowest privacy expectations, are preferred where viable. Level 4 imagery is subject to enhanced controls, including Inspecting-rank authorisation through the OIFR Submission Form process. Level 5 imagery is not used for OIFR. Decision-makers must also consider privacy expectations, human rights and equality impacts when selecting images and Image Reference Libraries, helping to ensure that OIFR Searches remain necessary and proportionate.

- **Intelligence status:** The Policy makes clear that a Potential Match or Viable Match constitutes an intelligence lead only and does not, by itself, justify arrest, search, detention or other enforcement action. Any subsequent policing activity must be lawful, necessary and proportionate and capable of independent justification.

- **Retention and deletion**: Image Reference Libraries are subject to defined ingestion, review and retention requirements. Temporary Libraries are made unavailable on expiry and deleted within 31 days. These controls reduce the risk of individuals remaining searchable through OIFR for longer than is necessary to achieve the relevant policing purpose.

- **Oversight and equality:** The FR Technology Board reviews usage and aggregated demographic data at least quarterly; annual public reporting supports accountability and PSED compliance.

4.11 In *Glukhin v Russia*, the European Court of Human Rights considered the use of facial recognition and wider surveillance technologies to identify, locate and arrest an individual through the coordinated use of large-scale CCTV infrastructure and facial recognition capability. The Court identified concerns regarding the breadth, intrusiveness and necessity of the measures used. The MPS's use of OIFR is

fundamentally different. OIFR may only be used in defined circumstances, for specified Use Cases, against Permitted Probe Subjects, and using authorised Permitted Image Reference Libraries. The acquisition of a Probe Image, the conduct of an OIFR Search and any subsequent use of the results are all subject to legal, operational and governance safeguards, including necessity and proportionality assessments, approval requirements, human review and defined retention and deletion requirements.

4.12 The MPS recognises that inclusion within a Permitted Image Reference Library and the use of facial recognition technology involve a greater degree of intrusion than traditional human-eye recognition because they require the processing of biometric data for the purpose of identifying individuals. However, OIFR also has the potential to provide a more targeted and less intrusive means of establishing or verifying identity than alternative policing methods which may otherwise be required. These may include prolonged detention whilst identity checks are undertaken, wider investigative enquiries, the obtaining of additional biometric modalities, or other resource-intensive methods of identification. The proportionality framework contained within the Policy requires decision-makers to consider the fair balance between the impact on individual rights and the anticipated policing benefit in each case. The safeguards set out above are intended to ensure that any residual impact on rights and freedoms is justified in all the circumstances having regard to the legitimate policing, safeguarding and risk-management benefits of OIFR.

2 Data Protection and 'Privacy Law' Assessment

Data Protection Act 2018 - Principle 1

1. The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

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 and either—
    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.

3. In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

4. […]
5. The second case is where—
    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
6. at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

Legal Risk: 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.

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.'

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

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.

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.

The MPS maintains and publishes an appropriate policy document as required by the DPA 2018.

Consent and the acquisition of Probe Images

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.

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

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.

Legal Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Legal framework If the processing lacks a lawful basis, individuals whose images are processed, whether as a Permitted Probe Subject or within a Permitted Image Reference Library, could be subject to unlawful interference with their rights. In the case of Permitted Probe Subjects, this interference may arise both from the acquisition of the Probe Image and from its subsequent biometric processing and	M	H	The following observations and risk mitigation points combine to ensure that the MPS processes data in a way which is compliance with the applicable legal framework. • **Legal Mandate and governance:** The MPS OIFR Legal Mandate sets out the lawful basis for using OIFR. This framework is implemented through the MPS OIFR Documents, notably the Policy, and at a search-specific level through the OIFR Submission Form, which records the applicable Use Case and the legal, necessity and proportionality assessment.	L	Ben Russell

Legal Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
comparison against a Permitted Image Reference Library. Unmitigated, such processing may undermine privacy expectations, particularly where individuals are unaware that their image has been obtained or may be subjected to biometric analysis. It may also adversely affect confidence in the use of facial recognition technologies and have a chilling effect on the willingness of some individuals to participate in lawful assemblies, express views publicly, associate with others, or otherwise exercise their rights to private and family life, freedom of expression, and freedom of assembly and association.			• **Part III DPA compliance:** All OIFR processing takes place under Part 3 DPA 2018. Where biometric data is processed for the purpose of uniquely identifying an individual, the processing constitutes sensitive processing under section 35(3) DPA 2018 and is undertaken in accordance with section 35(5), Schedule 8 and the MPS Appropriate Policy Document. • **Defined use cases:** Section 2 of the Policy restricts OIFR to specific Use Cases, ensuring that the capability is only used for legitimate law enforcement purposes and not for speculative or arbitrary biometric searching. • **Lawful acquisition of Probe Images:** The Policy restricts the circumstances in which Probe Images may be obtained. Under Use Case A, acquisition must take place either through the individual's real and informed consent or pursuant to a lawful common law policing power. Officers must satisfy themselves that the use of OIFR is lawful, necessary and proportionate in all the circumstances. • **Human rights and Equality Act considerations:** The Policy provides detailed proportionality guidance in relation to Articles 8, 9, 10, 11, and 14 ECHR. Each OIFR search requires consideration of these points, including whether less intrusive alternatives have been exhausted. • **Controls on image acquisition and use:** The Policy restricts both the acquisition and use of Probe Images. Annexes C and D impose enhanced safeguards where images engage elevated privacy expectations, wider human rights considerations, or involve children, disability or gender reassignment. • **Lawful investigative steps:** The Policy makes clear that a Potential Match or Viable Match constitutes an intelligence lead only and does not, by itself, justify arrest, search, detention or other enforcement action. Any subsequent activity must be independently justified and undertaken in accordance with the applicable legal powers. • **International Transfers:** OIFR outputs are not routinely transferred outside the United Kingdom. In the exceptional event that international law enforcement cooperation is required, any transfer will comply with the applicable requirements of Part 3 DPA 2018 and only the minimum data necessary for the relevant policing purpose will be disclosed. • **Oversight and accountability:** OIFR use is subject to audit, governance and oversight arrangements, including review through the FR Technology Board, monitoring of compliance with the Policy, and consideration of equality and human rights impacts.		
Accessibility & Foreseeability	M	M		L	

Legal Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Data subjects should be able to understand the framework governing the processing of their data and predict how it applies to them. Without this, there is a risk that the activity may not be considered "in accordance with law." For those whose images are processed—whether as a Probe Image or within an Image Reference Library—lack of transparency further risks individuals feeling unable to exercise their rights (including rights to assembly and expression, and individual data rights under the DPA 2018). This could undermine public trust and confidence in the MPS and its use of facial recognition technology.			The following observations and risk mitigation points combine to ensure that the MPS processes data in a way which is accessible and foreseeable to the public engaged by OIFR. • **Publication of governance documents**: The MPS publishes its OIFR Legal Mandate, this DPIA, and the wider OIFR Documents (including the Policy, Appropriate Policy Document, and Equalities Impact Assessment) on its website to ensure transparency and public accessibility. • **Clear legal and operational framework:** The Policy defines the circumstances in which OIFR may be used, the applicable Use Cases, the categories of Permitted Probe Subject, the Permitted Image Reference Libraries that may be searched, and the safeguards governing image acquisition, proportionality and authorisation. This assists individuals in understanding the circumstances in which OIFR may be ysed. • **Annual reporting and transparency measures**: Section 12 of the Policy requires the MPS to publish annual reports on the use of OIFR, including aggregated demographic analysis of searches undertaken, supporting accountability and foreseeability. • **Clear governance and oversight**: Internal oversight is provided by the FR Technology Board, which reviews usage and demographic data quarterly, ensuring compliance with legal and equality obligations.		Ben Russell

Fairness risk: The fairness of this activity needs to be considered, and mitigated in the context of data subjects.

Fairness Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Fairness – data processing Processing may be unfair where it is unwarranted, arbitrary or otherwise results in a disproportionate interference with the rights and freedoms of affected individuals, taking account of their reasonable expectations, the circumstances of the case and the purpose for which the processing is undertaken. For those whose images are contained within a Permitted Image Reference Library, there is a risk that the processing of their image for biometric identification purposes may affect their willingness to go about their daily lives, participate in lawful assemblies, associate with	M	H	The following observations and risk mitigation points combine to ensure that the MPS processes data which enables the MPS to achieve its policing objectives for OIFR but which is fair to data subjects. • **Published OIFR Documents**: The MPS OIFR Documents regulate and constrain the circumstances in which OIFR may be used. By publishing the Policy, DPIA, Appropriate Policy Document and Equality Impact Assessment, the MPS provides transparency regarding the use of OIFR and the safeguards governing its use. • **Transparency**: The MPS's commitment to transparency (Section 12 of the Policy) ensures that the use of OIFR is foreseeable to those whose images may be processed, whether as a Probe Image or within an Image Reference Library. Annual reports include aggregated demographic analysis of searches,	M	Ben Russell

Fairness Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
others, or otherwise exercise their rights to private and family life, freedom of expression and freedom of assembly and association. For Permitted Probe Subjects: • individuals may consider their privacy rights to be unfairly impacted if a Probe Image is obtained or subjected to OIFR without sufficient justification; • there is a risk that the acquisition of a Probe Image, particularly in circumstances involving elevated privacy expectations, may be perceived as intrusive or disproportionate; • there is a risk that individuals may consider the use of OIFR unfair if used in circumstances where less intrusive means of establishing or verifying identity were reasonably available; • there is a risk that concerns regarding the acquisition of images and biometric processing may have a chilling effect on individuals' willingness to participate in lawful activities, express views publicly, or associate with others. For both Permitted Probe Subjects and those whose images are contained within a Permitted Image Reference Library, there is a risk that OIFR may operate unfairly if it has a disproportionate impact on individuals sharing a Protected Characteristic, or if sufficient regard is not given to equality and human rights considerations when undertaking an OIFR Search.			supporting accountability and enabling individuals to exercise their rights under the DPA. • **Fairness 'by design'**: The MPS has published The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences, which explains the steps taken to quantify the statistical accuracy and demographic performance of its OIFR algorithm, including independent testing by the National Physical Laboratory (NPL). This testing confirmed a True Positive Identification Rate of 100% at Rank 1 with no statistically significant differences across race, gender, or age groups, ensuring equitable performance and reducing the risk of bias. • The NPL's findings, and wider support from MPS TRI has been reflected in the OIFR Policy, including operational guidance on image quality and system configuration to maintain fairness and accuracy and to assist those determining when there is a Viable Match. • **Controls on image acquisition and use:** The Policy strictly regulates the circumstances in which Probe Images may be acquired and used for OIFR. Under Use Case A, acquisition must take place either through real and informed consent or pursuant to a lawful common law policing power. The Policy also imposes controls through Annexes C and D where privacy, equality or wider human rights considerations arise. • **Image Tier controls:** Annex C applies a structured framework governing the acquisition and use of images. Enhanced safeguards, approvals and scrutiny apply where images engage elevated privacy expectations, equality considerations or wider human rights considerations. • **Protected characteristics safeguards**: Annex D provides additional safeguards and approval requirements in relation to children, disability, gender reassignment and other protected characteristics. These controls are intended to ensure that equality considerations are explicitly considered before OIFR is used. • **Search-specific considerations**: Every OIFR Search requires consideration of necessity, proportionality, equality impacts and, where applicable, whether non-OIFR alternatives have been exhausted or otherwise considered unviable in the circumstances. • **Ongoing reviews to mitigate risks of unfairness:** Informed by its Equality Impact Assessment, the MPS OIFR Documents provide for ongoing evaluation. This allows the MPS to monitor for equality and fairness issues by examining search outcomes and demographic trends. Concerns		

Fairness Risk	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			identified are escalated to the FR Technology Board for scrutiny and corrective action. • **Human review and Adjudication:** Any Potential Match returned by the OIFR System must be assessed by a trained OIFR User. OIFR does not determine identity through automated processing alone and any determination that a Viable Match exists requires human judgement. • **Ongoing review and monitoring:** Informed by the Equality Impact Assessment and operational performance data, the MPS monitors OIFR use to identify emerging fairness, equality or human rights concerns. Issues identified may be escalated through established governance arrangements for further scrutiny and corrective action. • **FR Technology Board Oversight**: The FR Technology Board reviews OIFR usage on at least a quarterly basis to monitor trends and direct changes for best practice. It also considers aggregated demographic data at these meetings to ensure compliance with the PSED. • **Training to ensure fairness**: OIFR Users receive training on the lawful acquisition of Probe Images, necessity and proportionality, equality and human rights considerations, Adjudication, and the limitations of facial recognition technology. Training assists users in avoiding unfair or discriminatory outcomes and ensures that Potential Matches are not treated as determinative of identity. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		

Data Protection Act 2018 - Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.					
Purpose limitation	**Likelihood** L/M/H	**Impact**	**Mitigations**	**Residual Risk** L/M/H	**MPS SRO** Sign Off
Processing images within an Image Reference Library for purposes beyond those for which they were originally collected or provided. OIFR involves the acquisition and processing of Probe Images and the use of images contained within Permitted Image Reference Libraries. There is a risk that either category of image could be processed for purposes beyond those for which their use was originally justified. In respect of Permitted Probe Subjects, there is a risk that a Probe Image obtained for a specific OIFR Use Case could subsequently be retained, reused or searched for a different purpose, resulting in processing that exceeds the scope of the original necessity and proportionality assessment. In respect of Permitted Image Reference Libraries, there is a risk that images could be used in support of OIFR Searches that fall outside the purpose for which the library was approved for use. This could result in individuals being subjected to biometric searching in circumstances that are inconsistent with the purpose for which the images were obtained and retained. More generally, there is a risk of function creep if OIFR is used outside the approved Use Cases, against individuals who are not Permitted Probe Subjects, or in circumstances that are not foreseen by the Policy. This could increase the privacy impact on affected individuals and undermine public trust and confidence in the use of OIFR.	L	M	The following observations and risk mitigation points combine to ensure that the MPS processes data in a way which complies with the purpose limitation principle. • **GDPR Exemptions**: In some circumstances, the DPA 2018 provides an exemption to particular UK GDPR provisions at Schedules 2 – 4 of the DPA. The main exemption of relevance to this point is the crime and taxation: general exemption. Sections 2 and Annex C (especially paragraph (b) of the Policy) support the use of the images and OIFR for law enforcement purposes (per Section 31). • **Use-Case Limitation**: The OIFR Policy (Section 2) restricts processing to two defined use cases. • **Permitted Probe Subject controls:** OIFR may only be used against Permitted Probe Subjects. This limits processing to those categories of individual specified within the Policy and reduces the risk of speculative or arbitrary biometric searching. • **Permitted Image Reference Library controls:** OIFR Searches may only be conducted against Permitted Image Reference Libraries authorised under Section 6 of the Policy. This helps ensure that images are used only for approved policing purposes and reduces the risk of function creep**.** • **OIFR Submission Form controls:** The requirement for an OIFR Submission Form provides an auditable record of compliance with the Policy and reduces the risk of secondary or unintended use • **RRD:** OIFR data is subject to defined retention and deletion requirements. These controls reduce the risk of information being retained and subsequently reused for purposes inconsistent with those for which it was originally obtained. • **Transparency and foreseeability**: The MPS publishes the OIFR Policy, DPIA, and Appropriate Policy Document online, and provides annual reporting on OIFR use. This helps ensure that the processing is foreseeable and accessible to the public, mitigating risks of unfairness or unexpected secondary use.	L	Ben Russell
Using OIFR for a different purpose	L	H	The following observations and risk mitigation points combine to ensure that the MPS will	L	Ben Russell

Purpose limitation	Likelihood L/M/H	Impact	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Section 2 of the Policy defines the only permissible Use Cases for OIFR, whilst Sections 4, 5 and 6 restrict how Probe Images may be acquired, who may constitute a Permitted Probe Subject, and which Permitted Image Reference Libraries may be used. There is a risk that OIFR could be used outside these defined parameters, or that the purpose for which a Probe Image was acquired could change after acquisition. Such processing may fall outside the reasonable expectations of affected individuals and reduce the foreseeability of OIFR use. Unmitigated, this could result in processing that is incompatible with the purpose for which a Probe Image was acquired or a Permitted Image Reference Library was authorised for use. It could contribute to function creep, speculative or repeated biometric searching, or the use of OIFR in circumstances not contemplated by the Policy. In turn, this may increase the privacy impact on affected individuals, adversely affect public confidence in the use of facial recognition technology, and have a chilling effect on the exercise of rights to private and family life, freedom of expression, and freedom of assembly and association. In more serious cases, use of OIFR for a purpose outside that permitted by the Policy could contribute to unlawful investigative activity or enforcement action based upon data processed for an incompatible or unjustified purpose			continue to process data which is compatible with the permissible use cases for OIFR: • **Policy controls:** The OIFR Policy defines the only permissible Use Cases for OIFR, the circumstances in which Probe Images may be acquired, the categories of Permitted Probe Subject and the Permitted Image Reference Libraries that may be used. The OIFR Submission Form process is structured around those requirements and does not permit arbitrary or unsupported uses of OIFR • **Fresh submission for any change:** OIFR Searches are justified by reference to a specific Use Case and necessity and proportionality assessment. Where the purpose underlying an OIFR Search changes, a fresh assessment and compliance with the Policy requirements are required, ensuring that processing does not continue on the basis of an outdated justification. • **Use Case, Probe Subject and Image Reference Library controls:** OIFR may only be used for an approved Use Case, against a Permitted Probe Subject and against an authorised Permitted Image Reference Library. These controls help ensure that processing remains aligned to the purpose for which OIFR use was justified and reduce the risk of function creep. • **Transparency of purpose:** The MPS publishes the OIFR Policy, DPIA, Appropriate Policy Document and associated governance documentation. Public reporting supports transparency, accountability and public understanding of the circumstances in which OIFR may be used. • **Technical and procedural safeguards:** Within the context of an OIFR Search, the MPS's approach to managing Permitted Image Reference Libraries ensures that images are enrolled, retained and used only for approved policing purposes. The governance arrangements applicable to each Image Reference Library help ensure that processing remains aligned to the authorised purpose of that library and reduces the risk of incompatible secondary use. • **Necessity and proportionality controls:** Every OIFR Search must be supported by a necessity and proportionality assessment, documented through the OIFR Submission Form process. This provides a case-specific safeguard against the use of OIFR for unrelated or unjustified purposes. • **Audit and oversight:** OIFR use is subject to audit, governance and oversight arrangements, including review through the FR Technology Board. These arrangements support compliance with purpose limitation requirements and enable concerns regarding		

Purpose limitation	Likelihood L/M/H	Impact	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			inappropriate use to be identified and addressed. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		

Data Protection Act 2018 - Principle 3

Personal data shall be adequate, relevant and limited to the necessities of the purposes for which they are processed.

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Too little / inadequate data If an OIFR Search is based upon data that lacks the minimum quality or quantity required for effective biometric comparison, there is a risk that the policing objective underlying the search will not be achieved. For individuals whose images are contained within a Permitted Image Reference Library, poor quality, outdated or otherwise unsuitable images may reduce the ability of the OIFR System to identify genuine matches, limiting the effectiveness of the capability. For Permitted Probe Subjects, poor image quality (for example low resolution, poor lighting, obstructions, unsuitable facial pose or insufficient facial detail) may prevent the generation of a Potential Match, result in the failure to identify a genuine	M	H	The following observations and risk mitigation points combine to ensure that the MPS has sufficient, suitable, but not too much data to effectively use OIFR. • **Image quality controls:** Annex C of the Policy establishes requirements governing the suitability and quality of Probe Images for OIFR use. OIFR Users are required to assess image quality before proceeding with a search and the OIFR System assists in identifying images that may be unsuitable for effective biometric comparison. • **Data Currency and Relevance:** Permitted Image Reference Libraries are derived from images lawfully held by the MPS and subject to defined governance arrangements. OIFR Users are required, so far as reasonably practicable, to utilise the most suitable and up-to-date Probe Image available in the circumstances. • **Ability to acquire a better Probe Image:** Where image quality issues are identified, and it is lawful and proportionate to do so, OIFR Users may obtain a further Probe Image to improve	L	Ben Russell

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
match, or reduce confidence in the outcome of an OIFR Search. Inadequate data may also require further image capture, repeated searches or reliance on alternative investigative methods, increasing the intrusion experienced by individuals whilst failing to achieve the intended policing purpose efficiently and effectively. For Use Case B, inadequate information concerning the identity, circumstances or risk profile of the detained individual may limit the ability of officers to properly assess whether an OIFR Search is necessary and proportionate. This could result in the use of OIFR without sufficient information to justify the search or to evaluate whether alternative measures would be capable of achieving the policing objective.			image quality and reduce the risk of unsuccessful or unreliable searches. • **Human review and Adjudication:** Any Potential Match returned by the OIFR System must be assessed by a trained OIFR User. Human Adjudication provides an additional safeguard where image quality, environmental conditions or other factors may affect confidence in the result and assists in identifying circumstances where the available data is insufficient to support a reliable outcome. • **Operational Guidance and Training:** OIFR Users receive training on assessing Subject, System, and Environmental factors that affect match viability, ensuring searches are based on adequate data. **Use Case B dataset controls:** Use Case B requires searching against an authorised Permitted Image Reference Library that has been selected because it is capable of providing information relevant to the detention, safeguarding and risk-management objective being pursued. The use of custody images and its associated police-held information helps ensure that the data available to decision-makers is capable of informing the assessment of risk and reducing the likelihood of decisions being made on the basis of incomplete or inadequate information. • **Similarity score threshold:** The OIFR System is configured with a similarity score threshold designed to reduce the impact of poor-quality or insufficient image data and minimise the return of irrelevant images 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. 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 • **Proportionality Checks:** The OIFR Submission Form requires consideration of whether non-OIFR alternatives have been exhausted, are otherwise considered unviable in the circumstances, or whether the use of OIFR is justified by Urgency. The assessment also requires consideration		

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			of whether the quality and quantity of available information are sufficient to justify the use of OIFR. • **Audit and Oversight**: The FR Technology Board reviews OIFR use, including trends relating to search outcomes, image quality issues and system performance, enabling operational learning and the identification of any issues affecting the adequacy or suitability of data used by the OIFR System. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		
Too much data processing There is a risk that an OIFR Search could involve the acquisition, processing or retention of more personal data than is necessary to achieve the relevant policing objective. For example: • acquisition of a Probe Image where less intrusive means of achieving the policing objective remain available or viable; • use of a Probe Image that contains more information than is necessary for the intended OIFR Search, including the processing of images depicting multiple individuals; • use of a more Permitted Image Reference Libraries than is necessary to achieve the relevant policing purpose; • repeated or unnecessary OIFR Searches in circumstances where the policing objective has already been achieved or where further searching is unlikely to provide additional value;	M	H	The following observations and risk mitigation points combine to ensure that the MPS has sufficient, suitable, but not too much data in order to effectively use OIFR. • **Rank 1 result presentation:** The OIFR System when used on a mobile device returns only the highest ranked result exceeding the applicable threshold for Adjudication. This reduces the amount of data presented to OIFR Users and assists in ensuring that only information necessary for the policing purpose is progressed. • **Strict Use-Case Limitation:** The Policy defines the only permissible Use Cases for OIFR. The OIFR Submission Form, records that the search is linked to a specific policing purpose and necessity case. • **Necessity and proportionality controls:** The Policy requires consideration of whether non-OIFR alternatives have been exhausted, are otherwise considered unviable in the circumstances, or whether the use of OIFR is justified by Urgency. OIFR may only be used where necessary and proportionate in all the circumstances. • **Permitted Probe Subject controls:** OIFR may only be used against Permitted Probe Subjects. This limits biometric processing to those individuals who satisfy the requirements of the Policy and reduces the risk of speculative or arbitrary searching.	M	Ben Russell

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
• retention of OIFR-generated data for longer than is necessary; • acquisition or use of images engaging elevated privacy expectations or protected characteristics without applying the enhanced safeguards required by Annexes C and D of the Policy. Unmitigated, this could result in excessive processing, unjustified collateral intrusion and a disproportionate interference with the rights and freedoms of affected individuals. It could also undermine public confidence in OIFR, create perceptions of function creep, and increase the risk of processing that is incompatible with the principles of necessity, proportionality and data minimisation.			• **Privacy-by-design ingestion:** Where multiple faces are present in a Probe Image, only the face selected and confirmed by the OIFR User as belonging to a Permitted Probe Subject proceeds to biometric comparison. This limits the processing of biometric data relating to third parties. • **Controls on image acquisition and use:** Annexes C and D impose additional safeguards where images engage elevated privacy expectations, wider human rights considerations, or involve children, disability or gender reassignment. Enhanced approval requirements apply in these circumstances. • **Permitted Image Reference Library controls:** OIFR Searches may only be conducted against Permitted Image Reference Libraries authorised under Section 6 of the Policy. Decision-makers must ensure that only those libraries necessary to achieve the relevant policing purpose are selected. • **Similarity score threshold:** The OIFR System is configured with a similarity score threshold designed to minimise the return of irrelevant images and reduce the likelihood of false matches being presented for Adjudication. The threshold is presently set at 6600 (0.66) and forms part of the MPS's data protection by design approach • **Retention, review and deletion:** OIFR data is subject to defined retention and deletion requirements. These controls reduce the risk of excessive retention and secondary use. • **Repeat search controls:** OIFR Searches should not be repeated unless there is a clear operational justification, such as new information, a material change in circumstances, improved image quality, or a new policing purpose capable of satisfying the Policy requirements. • **Oversight and audit:** OIFR use is subject to audit, governance and oversight arrangements, including review through the FR Technology Board. These arrangements assist in identifying excessive or unnecessary processing and support compliance with the data minimisation principle. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to		

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		
Irrelevant data processing There is a risk that OIFR may acquire, process or retain personal data that is not relevant to the policing purpose being pursued. This may occur where a Probe Image contains information unrelated to the intended OIFR Search, where images depicting individuals other than the Permitted Probe Subject are processed, or where OIFR Searches are conducted against Permitted Image Reference Libraries that are not necessary to achieve the relevant policing objective. Examples include: • acquisition or use of a Probe Image containing multiple individuals where only one individual is relevant to the policing purpose; • conducting an OIFR Search against more Permitted Image Reference Libraries than are necessary to achieve the policing objective; • repeated or speculative OIFR Searches without a clear operational justification; • processing images or information that are not relevant to the applicable Use Case, Permitted Probe Subject criteria, or the specific operational objective; • acquisition or use of images engaging elevated privacy expectations where the additional information contained within the image is not necessary for the intended OIFR Search. Unmitigated, this could result in the processing of personal data that is not relevant to the relevant policing purpose, creating unnecessary intrusion into private life, increasing the risk of collateral intrusion affecting third parties, and undermining public trust and confidence in the use of OIFR. It may also contribute to perceptions of function creep and reduce confidence that OIFR	M	H	The following observations and risk mitigation points combine to ensure that the MPS has relevant data for its purposes, and has minimised unnecessary data processing in so far as it can do so such that any remaining collateral intrusion is proportionate. • **Strict Use-Case Limitation:** The Policy defines the only permissible Use Cases for OIFR. Searches must be responsive to those Use Cases and supported by a completed OIFR Submission Form, which records the policing purpose, necessity case and proportionality assessment. This helps ensure that processing remains relevant to the policing objective being pursued. • **Permitted Probe Subject controls:** OIFR may only be used against Permitted Probe Subjects. This limits biometric processing to those individuals who satisfy the requirements of the Policy and reduces the risk of irrelevant or speculative searching. • **Permitted Image Reference Library controls:** OIFR Searches may only be undertaken against Permitted Image Reference Libraries authorised under Section 6 of the Policy. • **Controls on image acquisition and use:** Annexes C and D require consideration of privacy expectations, equality impacts and wider human rights considerations when acquiring and using Probe Images. Enhanced safeguards apply where images engage elevated privacy expectations or involve protected characteristics. • **Privacy-by-design ingestion:** Where multiple faces are present in a Probe Image, only the face selected and confirmed by the OIFR User as belonging to a Permitted Probe Subject proceeds to biometric comparison. This reduces the processing of irrelevant biometric data relating to third parties. • **Human-in-the-loop Adjudication:** Any Potential Match returned by the OIFR System must be assessed by a trained OIFR User. Adjudication assists in identifying and discarding results that do not meaningfully advance the policing purpose before any further action is taken. • **Similarity score threshold:** The OIFR System is configured with a similarity score threshold designed to minimise the return of irrelevant images and reduce the likelihood of unsuitable results being presented for Adjudication. The threshold has been informed by independent testing undertaken by the	M	Ben Russell

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
is being used in a necessary and proportionate manner.			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 limiting the results presented to OIFR Users to those exceeding the threshold, the system reduces the processing and consideration of images that are unlikely to be relevant to the policing purpose being pursued. 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. • **Repeat search controls:** OIFR Searches should not be repeated unless there is a clear operational justification, such as new information, a material change in circumstances, improved image quality, or a new policing purpose capable of satisfying the Policy requirements. • **Use Case B dataset controls:** Use Case B is undertaken against an authorised Permitted Image Reference Library selected because it may contain information relevant to the detention, safeguarding or risk-management objective being pursued, helping to ensure that OIFR is used against a dataset capable of advancing the policing purpose. • **Result Limitation:** When used on a mobile device, the OIFR System returns only the rank one result exceeding the applicable threshold for Adjudication. This limits the amount of personal data presented to OIFR Users and reduces the processing of information that is not relevant to the policing purpose. • **Oversight and Audit:** OIFR use is subject to audit, governance and oversight arrangements, including review through the FR Technology Board. These arrangements assist in identifying and addressing instances of irrelevant or unnecessary processing. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational		

Data minimisation	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		

Data Protection Act 2018 - Principle 4

Personal data shall be accurate and, where necessary, kept up-to-date and erased or rectified without delay.

Data accuracy	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Inaccuracies in the data itself Personal data processed through OIFR must be accurate and, where necessary, kept up to date, with processes in place to correct or remove inaccurate information. If inaccuracies occur, whether within a Probe Image, a Permitted Image Reference Library, associated metadata or records generated through an OIFR Search, there is a risk that the policing objective will not be achieved or that inappropriate decisions may be made. Examples include: • False negatives: Failure to identify a relevant individual because a Probe Image or Image Reference Library image is outdated, unsuitable or of insufficient quality. • False positives: The generation of a Potential Match that does not relate to the individual depicted in the Probe Image. • Inaccurate Adjudication: Errors in assessing a Potential Match as a Viable Match or in rejecting a genuine match. • Use Case B risk-management errors: Where information linked to an identified individual is inaccurate, incomplete or out of date, decisions	M	H	The following observations and risk mitigation points combine to ensure that the MPS has data with the necessary accuracy for its purposes without unduly impacting on the data subjects. • **Published Performance Data:** The MPS publishes information concerning the performance and governance of its facial recognition capability, supporting transparency and enabling ongoing scrutiny of accuracy and demographic performance. • **Training and Guidance for OFIR Users:** OIFR Users receive training on factors that affect match reliability, including image quality, time lapse, Subject, System and Environmental factors, and how those matters should be considered during Adjudication. • **Automated quality checks:** The OIFR System assists users in identifying poor-quality or otherwise unsuitable images before biometric comparison takes place. • **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	M	Ben Russell

Data accuracy	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
concerning detention, welfare, safeguarding or risk management may be based upon an incorrect understanding of the individual's circumstances. • Metadata inaccuracies: Incorrect date, time, location or contextual information associated with an image may result in the misinterpretation of OIFR results or inappropriate operational decisions. • Outdated reference imagery: Where images within a Permitted Image Reference Library no longer adequately reflect an individual's appearance, the effectiveness and reliability of OIFR may be reduced. Unmitigated, inaccuracies may adversely affect investigations, safeguarding activity, detention-related decision making, and wider operational activity. They may increase privacy intrusion, undermine public confidence in OIFR, result in unnecessary investigative activity, and in the most serious cases contribute to unlawful or unjustified operational decisions.			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. • **Periodic Oversight of Accuracy Trends:** The FR Technology Board monitors accuracy-related issues, including demographic performance, search outcomes and notable errors or trends, and may direct operational or technical changes where appropriate. • **Human-in-the-loop Adjudication:** Potential Matches are reviewed by trained OIFR Users before being deemed Viable Matches. This process considers image quality, time lapse, Subject, System and Environmental factors before any dissemination or operational reliance is placed upon the result. • **Image currency and suitability:** The Policy requires OIFR Users to ensure that Probe Images are suitable for the intended OIFR Search and comply with the requirements of Annex C. OIFR Users must consider image quality, age and suitability when determining whether to undertake an OIFR Search. Permitted Image Reference Libraries are subject to governance arrangements intended to maintain the suitability and currency of source imagery. • **Custody image safeguards:** Custody images used within Permitted Image Reference Libraries are subject to separate governance, retention and quality controls outside the OIFR System, helping to maintain the accuracy and integrity of the underlying image data. • **Accuracy of associated information:** Where a Viable Match is identified, information subsequently accessed by officers remains subject to existing MPS data quality, review and correction processes. This reduces the risk of operational decisions being informed by inaccurate or outdated information. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance		

Data accuracy	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		
Inaccuracies in algorithm Personal data processed through OIFR is compared using algorithmic similarity scoring. If the OIFR algorithm performs inaccurately, or if the system is configured inappropriately, this may adversely impact data subjects and operational integrity in several ways: • False or misleading Potential Matches: Inaccurate similarity scoring or inappropriate threshold settings may result in irrelevant candidates being presented for Adjudication, increasing the risk of disproportionate intrusion, unnecessary operational activity and erosion of trust. • False negatives: Genuine matches may not be returned by the system, reducing the effectiveness of OIFR and preventing the achievement of the underlying policing objective. • Failure to achieve policing objectives: If the OIFR System cannot reliably identify genuine matches, investigations, safeguarding activity, detention-related decision making and risk-management activity may be delayed or compromised. • Operational error propagation: Poor algorithm performance may amplify image quality issues, including poor lighting, occlusion, ageing, image resolution or facial pose, increasing the likelihood of unsuitable results being presented for Adjudication and requiring	M	H	The following observations and risk mitigation points combine to ensure that the MPS uses an algorithm with sufficient accuracy to achieve its policing objectives without unduly impacting individuals whose images are processed: • **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	L	Ben Russell

Data accuracy	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
additional officer time to assess. • Equality and fairness concerns: If system configuration or algorithmic performance were to produce materially different outcomes across demographic groups, there would be an increased risk of unfairness, indirect discrimination and non-compliance with the Public Sector Equality Duty. • Unnecessary biometric processing: Where algorithm performance is poor or system settings are inappropriate, OIFR may result in the processing and consideration of biometric data that is unlikely to advance the policing purpose, creating additional privacy intrusion without corresponding operational benefit. Unmitigated, this risk could adversely affect investigations, safeguarding activity and risk-management decisions, undermine public confidence in the use of OIFR, increase privacy intrusion, and in the most serious cases contribute to unlawful or unjustified operational decisions.			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. • **Repeat Search Discipline:** Repeat OIFR Searches are not undertaken routinely and should only occur where there is a clear operational justification, such as new information, improved image quality, a material change in circumstances, or a new policing purpose capable of satisfying the Policy requirements. • **Proof of Concept evaluation and performance monitoring:** OIFR is initially being deployed as a Proof of Concept and is subject to enhanced monitoring, audit and evaluation arrangements. The		

Data accuracy	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
			MPS will assess operational effectiveness, system performance, limitations, user compliance, privacy, equality and human rights impacts, complaints, legal challenges and public confidence considerations. Performance information, including Potential Matches, Viable Matches, operational outcomes and evidence of operational value, will be reviewed and reported to the MPS Facial Recognition Technology Board. These arrangements provide an additional safeguard by enabling the MPS to identify issues, assess whether safeguards are operating effectively and determine whether OIFR should be modified, restricted, expanded or discontinued		

Data Protection Act 2018 - Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose for which it is processed.

Record review, retention and deletion	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Data retention There is a risk that, if the retention periods set out in the Policy are not applied and data is not subject to meaningful review, personal data processed through OIFR could be retained beyond its operational necessity. This may have a number of impacts: • **Undue processing:** Retaining Probe Images, biometric templates, OIFR Submission Forms, Match Reports or other OIFR-generated records for longer than necessary may increase privacy intrusion and create opportunities for secondary, unexpected or speculative use. • **Expanded exposure:** Personal data retained without a continuing policing purpose may be exposed to a greater risk of inappropriate access, disclosure or use, undermining proportionality and fairness. • **Retention of biometric data:** OIFR involves the processing of biometric	M	H	The following observations and risk mitigation points combine to ensure that the MPS has balanced its need for retention of data with the risks and impacts of doing so. • **Published retention periods:** Data is processed in accordance with Part III DPA 2018 and subject to the retention, review and deletion requirements set out in Section 11 of the OIFR Policy. • **Review and deletion controls:** OIFR-generated data is subject to review and deletion requirements designed to ensure that information is not retained beyond its operational relevance. Where the relevant policing purpose has been achieved, data is deleted in accordance with the Policy. • **Proof of Concept retention safeguards:** During the Proof of Concept, data generated through OIFR Searches may be retained for testing, evaluation and performance monitoring purposes. Such retention is time limited, subject to governance controls, and followed by deletion in accordance with the Policy once evaluation and audit requirements have been completed. • **Restricted access controls:** Access to retained OIFR data is limited to authorised personnel with a legitimate operational, governance, audit, testing or system support requirement. This	L	Ben Russell

Record review, retention and deletion	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
data for the purpose of uniquely identifying individuals. Retaining records generated through that processing beyond necessity may increase the impact on affected individuals' rights and freedoms. • **Function creep:** Retained OIFR records may be used for purposes that were not contemplated when the original OIFR Search was undertaken, reducing confidence that the capability is being used only for defined policing purposes. • **Loss of public trust:** Extended retention without adequate justification may erode confidence in the MPS and its use of facial recognition technology, particularly where individuals believe that images acquired for a specific operational purpose continue to be held unnecessarily. • **Operational inefficiency:** Failure to review and delete data may result in unnecessary processing, increased governance burdens and the retention of information that no longer assists the relevant policing purpose. Unmitigated, this risk could compromise compliance with Part 3 DPA 2018, increase privacy intrusion, undermine the principles of necessity and proportionality, and damage public confidence in OIFR and wider policing activity.			reduces the risk of retained information being accessed or used unnecessarily. • **Audit and oversight:** Audit logs record actions relating to the retention, review and deletion of OIFR data. Compliance with retention requirements is monitored through established governance arrangements, including oversight by the FR Technology Board where appropriate. • **Retention linked to policing purpose:** Retention periods are linked to defined operational and governance requirements, helping to ensure that personal data is not retained once the justification for its continued retention no longer exists. • **Individual rights compliance:** The MPS facilitates the exercise of applicable individual rights under Part III DPA 2018 and maintains processes for the correction, deletion and review of personal data where required by law.		

Data Protection Act 2018 - Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data compromise	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Data security People's privacy and wider interests may be compromised if personal data processed through OIFR is not protected by robust technical and organisational security measures against internal and external threats. The use of a proprietary facial recognition algorithm and third-party suppliers may introduce security risks, including confidentiality breaches, system vulnerabilities, supply chain compromises, or insufficient contractual and governance controls. Such risks could affect the confidentiality, integrity and availability of personal data and undermine lawful processing. For individuals whose biometric data is processed, whether as part of an Image Reference Library or a Probe Image, the unique nature of biometric identifiers means that, if a security breach occurs, the data could be exploited by malicious actors. Unlike many other forms of personal data, biometric characteristics cannot readily be replaced or changed if compromised. For individuals represented within an Image Reference Library or who are the subject of a Probe Image, a security breach could reveal that their data was processed for a law enforcement purpose and, potentially, in connection with a particular OIFR use case or criminal investigation. This could expose sensitive operational information, prejudice policing activity, and adversely affect the individual concerned if the information were misused or inappropriately disclosed.	L	H	The following observations and risk mitigation points combine to ensure that the MPS has mitigated the risks regarding Data Security. • **Security Framework:** Section 11 of the OIFR Policy sets out the technical and organisational measures adopted to secure OIFR data processing. • **Access Controls:** Role-based access ensures only authorised personnel can interact with OIFR systems and data. • **Personnel Security:** All staff involved in OIFR processing undergo appropriate vetting checks. • **Training:** MPS baseline data protection and information security training is mandatory for all personnel handling OIFR data. • **System Design:** Biometric templates generated by OIFR are algorithm-specific and cannot be universally applied, reducing the risk of misuse outside the system. • **Security Against Unlawful Processing:** OIFR governance documents define structures to record OIFR Searches, approval of them and oversight. OIFR Users are subject to clear disciplinary processes be it as police officers or police staff. • **OIFR Supplier:** The supplier is subject to confidentiality and security safeguards as part of the contractual arrangements. The supplier does not have access to personal data processed by the MPS within the OIFR system. • **Audit and Monitoring:** Audit logs capture processing actions. Periodic audits and post-use reviews (at least quarterly) by the FR Team provide assurance and identify lessons learned. • **Encryption and Secure Storage:** All biometric and associated data is encrypted, with secure storage protocols aligned to MPS standards.	L	Ben Russell
Data loss If data processed by OIFR becomes inaccessible or is corrupted—whether through	M	M	The following observations and risk mitigation points combine to ensure that the MPS has mitigated the risks which arise from potential	L	Ben Russell

Data compromise	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
unlawful action, technical failure, or accidental deletion—it may undermine the ability to conduct retrospective facial recognition searches. This could prevent the MPS from progressing investigations, acting on matches, or reporting on the outcomes of OIFR use. Loss of data may also compromise investigation integrity and operational accountability. It may also prevent the MPS acting on, and reporting on the use of OIFR.			data loss in order to ensure OIFR remains a functional capability. • **Business Continuity Planning:** The MPS maintains business continuity plans to ensure continued operational capability in the event of system failure or data loss. These plans apply to OIFR processes. • **System Backups:** The OIFR system is backed up. Wider back up and continuity arrangements are in place for systems which support Image Reference Libraries (e.g. custody images). • **Redundancy Measures:** OIFR systems are designed with failover and recovery protocols to minimise downtime and ensure continuity of investigative processes. • **Controlled Data Handling:** Authorised personnel follow designed-in processes flows for data ingestion and export, reducing the risk of accidental deletion or corruption. • **Audit and Monitoring:** Audit logs track processing activity, enabling rapid identification and remediation of anomalies. • **Secure Storage:** All OIFR data is stored in secure environments with encryption at rest and in transit, reducing vulnerability during recovery operations.		

Complaint Handling

Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection Officer (DPO).

Complaints about the use of Personal Information in relation to this project should be handled through the Data Office overseen by the MPS Data Protection Officer (DPO).

Freedom of Information Act 2000 (FOIA)

In meeting its FOIA obligations, the MPS is committed to maintaining an open and transparent approach regarding the processing outlined within this DPIA. This is subject to any exemptions that may apply under FOIA, including those relating to security or confidentiality.

The MPS is a public authority for the purposes of the FOIA. This means that information held by the MPS is accessible to the public on written request, subject to limited exemptions.

In accordance with guidance from the ICO, the MPS will place this DPIA and other associated MPS RFR Documents onto our FOIA Publication Scheme, helping to raise public awareness of how the MPS processes personal data. Any exception to this will meet FOIA criteria.

All public requests for information should be directed through Communication & Engagements triage team, overseen by the MPS DPO.

3 Individual Rights

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Right to be informed Unless an exemption applies under Part 3 DPA 2018, individuals have a right to receive information about how the MPS processes their personal data. This includes information concerning the purposes of processing, the legal basis relied upon, retention arrangements, recipients of personal data and the rights available to data subjects. OIFR presents particular transparency considerations because it involves both the acquisition of Probe Images and the subsequent processing of biometric data for the purpose of identifying an individual. Depending on the circumstances, individuals may not always be aware that their image has been acquired, submitted for an OIFR Search, or compared against a Permitted Image Reference Library. This risk is heightened where a Probe Image is acquired without the individual's knowledge, as the absence of awareness may reduce transparency, limit the individual's ability to understand how their personal data is being processed, and increase perceptions that OIFR is operating in a manner analogous to covert information gathering or surveillance.	M	M	The following observations and risk mitigation points combine to ensure that the MPS has mitigated the risks which arise from any impact • **MPS Governance:** The MPS maintains established information governance, data protection and accountability arrangements which support transparency in the processing of personal data and the protection of individual rights. OIFR operates within those wider governance arrangements and the safeguards contained within the Policy. • **Publication and accessibility:** The MPS publishes its Privacy Notice, Appropriate Policy Document, OIFR Policy, DPIA and Equality Impact Assessment. These documents explain the circumstances in which OIFR may be used, the safeguards governing its deployment, and the rights available to affected individuals. This assists in ensuring that the operation of OIFR is accessible and foreseeable. • **Transparency requirements:** Section 12 of the Policy contains specific transparency requirements applicable to OIFR. These requirements assist in ensuring that information concerning the existence, operation and safeguards of OIFR is made available to the public, subject to any applicable operational or statutory exemptions. • **Consent and transparency:** Under Use Case A, where practicable and consistent with operational objectives, consent should be sought before reliance is placed on a common law power to obtain a Probe Image. This promotes transparency and supports the	M	Ben Russell

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Unless an exemption applies, a failure to provide sufficient information regarding the use of OIFR may prevent individuals from understanding how and why their personal data is being processed, inhibit the exercise of rights under Part 3 DPA 2018, and undermine the accessibility and foreseeability of the OIFR regime. It may also reduce public confidence in the MPS and its use of facial recognition technologies. For individuals whose images are contained within a Permitted Image Reference Library, a lack of transparency may create uncertainty regarding the circumstances in which those images may be searched using OIFR. For Permitted Probe Subjects, insufficient information regarding the acquisition of images and subsequent biometric processing may increase the perception that OIFR is being used in an arbitrary or disproportionate manner. Unmitigated, these issues may undermine public trust and confidence, inhibit the exercise of individual rights and increase the risk that OIFR is perceived as operating in a manner that is insufficiently transparent, foreseeable or accountable.			individual's understanding of how their image may be used and processed. • **Use Case B safeguards:** Where OIFR is used, its use remains subject to the transparency and information requirements contained within the applicable statutory framework, codes of practice and operational procedures governing the underlying power. These requirements provide an additional safeguard by ensuring that OIFR is deployed within an established legal and regulatory framework that is published and already subject to scrutiny and oversight. • **MPS Policy and Guidance:** The MPS Data Office provides advice and guidance regarding compliance with data protection obligations, including transparency requirements and the exercise of individual rights under Part III DPA 2018. • **The DPO Role:** The MPS DPO provides advice, challenge, oversight and assurance in relation to the processing of personal data through OIFR. The DPO also supports compliance monitoring and the exercise of individual rights. • **FR Technology Board Oversight:** The FR Technology Board provides oversight of OIFR use, including consideration of governance, transparency, equality impacts, compliance and public confidence. • **Proof of Concept transparency:** Annex E provides for the monitoring and evaluation of OIFR during the Proof of Concept and requires the outcome of the pilot to be reported to the FR Technology Board and published on the MPS website. This supports accountability, public understanding and scrutiny of the capability. • **Individual rights framework:** The MPS facilitates the exercise of applicable rights under Part III DPA 2018 and maintains processes for responding to enquiries, complaints and requests relating to the processing of personal data through OIFR.		

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Right of Access Unless there is an exemption, not only do individuals have a right to be aware of the data held and being processed about them, in normal circumstances they have a right to verify this too by seeking access to the data the MPS holds on them. When designing the project there is a need to think about how it will	M	L	The following observations and risk mitigation points combine to ensure that the MPS has facilitated the exercise of individual rights and mitigated the risks which arise from any impact from a failure to do so. • **Systems Capability:** OIFR systems are designed to enable deletion or restriction of data in response to valid data subject rights requests under the DPA 2018. This includes the ability to remove Probe Images or entries from	L	Ben Russell

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
enable people to access their data – from having systems to ensure the Data Office come to those responsible for the Project with requests to how data is extracted from the Project to be shared with the individual.			Image Reference Libraries where appropriate. • **Retention Controls**: OIFR processes incorporate retention safeguards. Data is only held for defined periods (as set out in Section 11 of the RFR Policy) and is subject to periodic review and deletion when no longer operationally relevant. This reduces the need for erasure requests by ensuring proactive deletion. • **Proof of Concept controls:** During the Proof of Concept, retained data remains subject to the governance, access control, evaluation and deletion arrangements contained within Annex E. This helps ensure that data retained for testing, audit or evaluation purposes remains subject to appropriate safeguards and oversight. • **Privacy Notice**: This provides that requests for data erasure or restriction may be considered via: DataProtectionOfficer@met.police.uk or via post to MPS Data Rights, PO Box 313, Sidcup, DA15 0HH. • **MPS website**: This provides the public with a copy of the MPS Privacy Notice that details how the right to erasure or restriction may be exercised. • **MPS OIFR Documents**: These provide detailed safeguards around the use of data and how it will be held and managed. • **MPS policy**: and guidance is provided by the MPS's Data Office to ensure the MPS complies with this legal obligation. • **Training and awareness of individual rights:** OIFR Users receive training on data protection obligations and the rights available to data subjects under Part III DPA 2018. This includes understanding how individuals may exercise those rights and the role of OIFR records, including OIFR Submission Forms and Match Reports, in supporting the MPS's response • **The DPO Role**: The MPS DPO is an integral role to the processing of personal data and the upholding of individual rights, providing scrutiny, challenge, advice to do so.		
Right of Rectification If data is not up to date, there is a risk that decisions are being made on the basis of inaccurate information. If inaccuracy becomes apparent, or, if an individual requests correction, systems need to be in place to update (or add to incomplete) information.	L	L		L	Ben Russell
Right of Erasure and Restriction Individuals have a right to request the deletion or removal of their personal data. They also have a right to block or restrict processing their data going forwards. This request is subject to exemptions to ensure it cannot be used to frustrate policing purposes, or where the request is manifestly unfounded or excessive. However, the Project team does need to ensure there are systems in place to be able to delete data on request and to restrict its further processing. A failure to have systems in place risks individuals losing confidence in the MPS holding only the data it needs and being unresponsive to their lawful requests.	L	M		M	Ben Russell

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Right not to be subject to automated processing Part III of the DPA 2018 provides safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. without human intervention.	L	M	The following observations and risk mitigation points combine to ensure that the MPS has mitigated the risks which arise: • **Adjudication**: OIFR does not make decisions that produce adverse legal effects or significantly affect individuals without human intervention. Any match generated by OIFR is subject to mandatory adjudication, ensuring human-in-the-loop assessment before	L	Ben Russell

Individual right	Likelihood L/M/H	Impact L/M/H	Mitigations	Residual Risk L/M/H	MPS SRO Sign Off
Individuals have the right not to be subject to a decision when: • it is based on automated processing; and • it produces an adverse legal effect or a significantly affects the individual.			any operational decision is taken. Investigators review the match, consider its context, and apply professional judgment to determine whether further action is appropriate. The OIFR system itself does not autonomously trigger any enforcement or engagement.		

4 Conclusion

4.1 The DPIA has identified a number of relevant risks associated with the use and security of imagery, the use of OIFR, and the post-processing phases relating to OIFR results.

4.2 Proportionate and reasonable mitigations have been identified and fall within the guidelines associated with the OIFR operating principles. Whilst no exceptional areas of risk have been identified at present, this DPIA is a living MPS document and will be subject to continuous review. This DPIA is also subject to case-specific considerations documented in the relevant OIFR governance forms.

4.3 This DPIA complies with the requirements of the DPA 2018.

5 Data Protection Impact Assessment Sign-off

DPIA Signature

1.	**Project Sponsor**
	Sign Below:
	Name:
	Position: DAC
	Date: [XXX]
2.	**Data Protection Officer**
	I have assessed this DPIA in conjunction with the accompanying Policy, Equality Impact Assessment, Legal Mandate and Appropriate Policy Document, it is clear that substantial consideration of Part 3 of the Data Protection Act 2018, together with the obligations arising from the Human Rights Act 1998 and Equality Act 2010 have been considered; identifying the high-risk nature of facial recognition processing arising from the Proof of Concept use of Operator Initiated Facial Recognition (OIFR), and the potential impact on individuals' rights and freedoms. The following recommendations are made to strengthen assurance and support ongoing compliance: i) **Define explicit DPIA review triggers.** Whilst the DPIA and the associated Policy provide for ongoing review, the SRO should consider documenting within

the Policy at *Annex E(b)*, the specific triggers such as material technology changes, new use cases, equality concerns, significant complaints, audit findings or personal data breaches- so it is clear what may trigger a review.

ii) **Introduce periodic quality assurance of OIFR Submission Forms and associated transparency requirements.** The Policy clearly requires completion and oversight of Submission Forms at *Annex E(f)(i)*, periodic sampling and review would provide assurance that necessity, proportionality, alternative options, image selection, transparency obligations, and authorisation requirements are being applied consistently.

iii) **Maintain oversight of enhanced safeguards for higher-risk cases and user competency.** The DPIA records risks and mitigations, and the Policy contains additional approval and safeguarding requirements relating to children, vulnerable individuals and other elevated-privacy or equality risk scenarios. Formal governance review, *Annex E(e)* within the Policy should reference specifically that oversight controls for children and vulnerable individuals will be a part of the assurance process in practice.

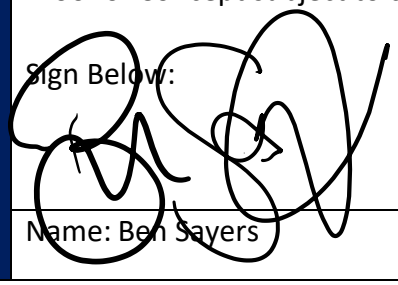
The SRO and Information Asset Owner (if different from the SRO) must maintain appropriate accountability arrangements for this processing, including ensuring that relevant ROPA records remain accurate, that pilot outcomes, audit findings, training compliance, retention and deletion compliance, and equality monitoring are actively reviewed through established governance channels.

Subject to this advice and recognising that this DPIA is intended to remain a living document subject to ongoing review, I am satisfied that the identified risks have been appropriately considered and mitigated to a level that does not currently indicate a need for prior consultation with the ICO.

However, if the Proof of Concept identifies unexpected demographic disparities, significant accuracy issues, material changes to the technology or use cases, serious compliance concerns, personal data breaches, legal challenge, or evidence that the identified mitigations are not operating effectively, the DPIA should be reviewed, the DPO engaged, and the need for consultation with the ICO reconsidered.

On that basis, I recommend approval of the DPIA and support progression of the Proof of Concept subject to continued monitoring and oversight.

Sign Below:



Name: Ben Sayers

	Position: DPO
	Date: 05 November 2026

Change control:

Version	Date	Authority	Evidence of approval	Record of change
1.0	1 November 2027	SRO	Sign off	New version

6 Protective Marking

Classification	Official
Suitable for Publication	Yes
Title	DPIA relating to the use of Operator Initiated Facial Recognition by the MPS.
Purpose	To cover privacy issues and mitigate risks arising from use of Operator Initiated Facial Recognition.
Author	MPS OIFR
Version	1.0
Creating Unit	MPS OIFR
Date Created	1 November 2026
Review Date	1 November 2027