METROPOLITAN POLICE

More Trust | Less Crime | High Standards

Protective marking:	Official
Publication scheme Y/N:	No
Title:	OFFICER INITIATED FACIAL RECOGNITION: LEGAL MANDATE
Version:	1.0
Summary:	Outlines the legal basis for the MPS's use of OIFR technology to assist in identifying unknown subjects, confirming or disproving the identity of known subjects, and establishing whether images of a subject are held within a Permitted Image Reference Library, for the purposes of preventing and detecting crime, safeguarding vulnerable persons, and supporting policing investigations and operations.
Branch/ OCU:	MPS DLS
Review date:	November 2027

MPS OFFICER INITIATED FACIAL RECOGNITION: LEGAL MANDATE

Contents

1. **Introduction** 2
2. **Purpose of OIFR** 3
3. **The Benefits of OIFR** 3
4. **Legal Context** 3
5. **MPS OIFR Policy** 9
6. **Human Rights Act 1998** 9
7. **Equality Act 2010** 16
8. **Data Protection Act 2018** 17
9. **Legal Considerations Regarding Using OIFR in relation to the Deceased** 19
10. **Freedom of Information Act 2000** 21
11. **Impact Assessments** 21

This legal mandate will be subject to periodic review, on at least an annual basis. It can be amended as the law and technology develops further, or as matters relating to Officer Initiated Facial Recognition (OIFR) evolve. It is anticipated that circumstances may arise which fall outside of the scope

of this legal mandate. In such circumstances legal advice should be sought from the Directorate of Legal Services.

1. Introduction

1.1. The Metropolitan Police Service ("MPS") considers that OIFR is capable of being used lawfully in support of the policing functions entrusted to it. The legal basis for OIFR derives from a combination of common law policing powers, statutory powers authorising the obtaining and retention of photographs, and the safeguards imposed by the Human Rights Act 1998, the Data Protection Act 2018, the Equality Act 2010 and other applicable legislation. OIFR is an overt facial recognition capability that enables an authorised OIFR User to compare a Probe Image depicting a Permitted Probe Subject against the Permitted Image Reference Library for a specified policing purpose.

1.2. The lawfulness of any use of OIFR depends not only upon the existence of a lawful policing purpose, but also upon compliance with the restrictions, safeguards and governance measures contained within the OIFR Policy and associated OIFR Documents.

1.3. This Legal Mandate must be read alongside the MPS OIFR Documents:

(i) OIFR Policy;

(ii) OIFR Data Protection Impact Assessment;

(iii) OIFR Appropriate Policy Document;

(iv) OIFR Equality Impact Assessment;

(v) MPS Facial Recognition Technology: Understanding Accuracy and Demographic Differences; and

(vi) Applicable MPS training and governance documentation.

1.4. This Legal Mandate explains the legal basis upon which the MPS may:

(i) Acquire and process Probe Images;

(ii) Use Image Reference Libraries;

(iii) Generate Potential Matches;

(iv) Determine whether a Potential Match constitutes a Viable Match; and

(v) Make lawful operational use of information arising from OIFR Searches.

1.5. OIFR is initially being deployed as a Proof of Concept. The operational limitations, evaluation requirements and governance arrangements applicable to the Proof of Concept are set out in Annex E of the OIFR Policy.

2. Purpose of OIFR

2.1. The MPS may only use OIFR for the Permitted Use Cases contained within the OIFR Policy.

2.2. Pursuant to Use Case A, OIFR may be used:

(i) a subject's identity is unknown; or

(ii) there are reasonable grounds to doubt a subject's claimed identity, and

establishing that subject's identity is necessary for a law enforcement purpose

2.3. Pursuant to Use Case B, OIFR may be used where:

(i) A person has been lawfully arrested or otherwise detained; and

(ii) A statutory power exists to obtain that person's photograph.

2.4. The purpose of Use Case B is to support the safe and effective management of arrested or otherwise detained persons. OIFR may assist in establishing identity, identifying aliases, false identities and warning markers, and identifying information relevant to safeguarding, vulnerability, self-harm, violence, officer safety and wider risk-management considerations which may not otherwise be identified through biographical enquiries alone.

3. The Benefits of OIFR

3.1. The MPS's view is that OIFR is an effective and valuable tool which enhances the use of still images and video imagery across investigative and operational activity. It forms part of a wider suite of technical and operational capabilities used nationally and within the MPS, including the Police National Database (PND), Automated Number Plate Recognition (ANPR), Closed-Circuit Television (CCTV) and Body-Worn Video (BWV), to prevent and detect crime, safeguard vulnerable persons and support the discharge of policing functions.

3.2. The MPS considers that OIFR may provide a number of operational benefits, including:

(i) identifying unknown subjects;

(ii) verifying disputed or uncertain identities;

(iii) generating intelligence leads which may assist investigations and policing operations;

(iv) supporting safeguarding activity and the protection of vulnerable persons;

(v) supporting risk assessment and risk management, including in relation to officer and public safety;

(vi) supporting timely and informed operational decision-making;

(vii) reducing reliance on more intrusive methods of establishing identity, including arrest, detention and the collection of additional biometric data where lawful alternatives are available; and

(viii) improving investigative efficiency and reducing delays in progressing investigations and operational activity.

4. Legal Context

The applicable legal framework

4.1. The use of OIFR by the MPS is governed by a combination of common law powers, statutory provisions and legal safeguards rather than a single statutory regime. Collectively, these requirements, including obligations arising under human rights, data protection and equality legislation, establish the legal framework for OIFR Searches, including the circumstances in which they may be conducted, the images that may be used, and the safeguards that apply throughout the use of OIFR.

The legal basis for OIFR

4.2. The use of OIFR by the MPS is not governed by a single statutory regime. Rather, OIFR operates within a framework comprising of:

(i) Common law policing powers;

(ii) Statutory powers relating to the acquisition and use of photographs;

(iii) The Human Rights Act 1998;

(iv) The Equality Act 2010;

(v) The Data Protection Act 2018;

(vi) Relevant Codes of Practice;

(vii) Judicial authority concerning the acquisition, retention and use of photographs and facial recognition technologies; and

(viii) The MPS OIFR Documents.

4.3. The legality of any OIFR Search must be assessed against this framework as a whole.

4.4. As a police service, the MPS has a number of long-established policing responsibilities and powers derived from the common law, which have been consistently recognised by the courts. The MPS relies upon those powers in carrying out its policing functions and in exercising a range of investigative, safeguarding and public protection responsibilities.

4.5. Key common law powers relied upon by the MPS include (but are not limited to) powers including, the prevention and detection of crime, the investigation and prosecution of offences, the protection of life, property and public safety, the safeguarding of vulnerable persons, and the protection of national security. These common law policing powers form an important part of the legal foundation supporting the acquisition of Probe Images, the maintenance and use of Permitted Image Reference Libraries, and the conduct of OIFR Searches.

4.6. The courts have expressly recognised the ability of police forces to rely upon established common law policing powers when deploying facial recognition technologies. In *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 ("*Bridges")*, the Court of Appeal accepted that police forces are capable of relying upon existing policing powers when using facial recognition technologies and did not require a bespoke statutory power authorising facial recognition in every circumstance. The Divisional Court had previously concluded that the police's common law powers were "amply sufficient" to support the use of facial recognition technology and that the police did not require new express statutory powers for such purposes.

4.7. Whilst *Bridges* concerned Live Facial Recognition rather than OIFR, the principles identified by the Court are equally applicable. The use of facial recognition technology must be supported by a sufficiently accessible and foreseeable legal framework and be subject to appropriate safeguards.

4.8. The MPS considers that OIFR operates within such a framework, comprising common law policing powers, applicable statutory powers relating to imagery, the law enforcement provisions of Part 3 of the Data Protection Act 2018, and the safeguards contained within the OIFR Policy Documents.

4.9. Accordingly, an OIFR Search may only be conducted where it is for a Permitted Use Case, concerns a Permitted Probe Subject, utilises a lawfully acquired Probe Image and a Permitted Image Reference Library, complies with the requirements relating to imagery and protected characteristics, is necessary and proportionate in all the circumstances, and is undertaken in accordance with the applicable governance, audit, retention and transparency requirements.

Acquisition and Use of Probe Images

General principles

4.10. OIFR operates by comparing a lawfully held Probe Image against images accessible through approved police systems. The lawfulness of an OIFR Search therefore depends not only upon a lawful basis for the search itself, but also upon the lawful acquisition, retention and processing of the Probe Image.

4.11. The legal basis for obtaining and retaining a Probe Image will depend upon the circumstances in which it was acquired. Officers must be satisfied that any image used for OIFR purposes has been lawfully obtained, retained and processed in accordance with applicable legal requirements.

4.12. The existence of a lawful basis to obtain or retain an image does not, of itself, authorise its use in OIFR. Any decision to conduct an OIFR Search remains subject to separate considerations of legality, necessity and proportionality.

Use Case A

4.13. Under Use Case A, OIFR may be used where the identity of a subject is unknown, or there are reasonable grounds to doubt an identity attributed to that subject, and identification is necessary for a law enforcement purpose.

4.14. Any Probe Image used for Use Case A must be lawfully obtained. A Probe Image may be acquired with the individual's informed consent or pursuant to a lawful common law policing power. Where a Probe Image is obtained pursuant to a common law power, the officer must be lawfully present at the location where the image is obtained, obtain the image overtly, and be readily identifiable as a police officer. Where practicable to do so without compromising operational objectives, consent should be sought before any common law power is used. However, the refusal or withdrawal of consent does not, of itself, prevent the acquisition of a Probe Image pursuant to an otherwise lawful policing power.

4.15. The MPS recognises that interactions between police officers and members of the public may raise questions as to whether consent is freely given. Accordingly, whilst consent may be relevant to the lawful acquisition of a Probe Image and to the assessment of proportionality, the MPS does not rely upon consent as the legal basis for the subsequent biometric processing undertaken through OIFR. Rather, OIFR Searches are conducted pursuant to the wider law enforcement framework described in this Legal Mandate and Part 3 of the Data Protection Act 2018.

Use Case B

4.16. Under Use Case B, Probe Images are obtained pursuant to statutory powers (detailed within the below paragraphs) authorising the taking of photographs from arrested, detained, or otherwise lawfully processed individuals.

4.17. Use Case B is intended to support the safe and effective management of such individuals by facilitating the identification of information relevant to identity, safeguarding, vulnerability, self-harm, violence, officer safety, and wider risk-management considerations at the earliest practicable opportunity.

4.18. The existence of a statutory power to obtain a photograph does not, of itself, authorise an OIFR Search. Any such search constitutes separate biometric processing and must comply with this Legal Mandate, the OIFR Policy, and the wider legal framework governing law enforcement processing.

Police and Criminal Evidence Act 1984

4.19. Section 64A of the Police and Criminal Evidence Act 1984 ("PACE") provides a statutory basis for the acquisition, retention and use of photographs that may subsequently be utilised as Probe Images within OIFR.

4.20. Section 64A(4)(a) provides that photographs obtained under that power may be used or disclosed for purposes related to the prevention or detection of crime, the investigation of offences, the conduct of prosecutions, and the enforcement of sentences. The MPS considers that those statutory purposes are capable of encompassing the retention and use of photographs within the OIFR framework.

4.21. PACE Code D further recognises a range of identification-related policing purposes for which photographs may be used, including establishing or verifying identity, determining whether an individual is wanted, supporting criminal investigations, assisting in identification procedures, and supporting the apprehension and management of offenders.

4.22. Whilst the purposes identified within section 64A PACE and PACE Code D are closely aligned with a number of the objectives served by OIFR, the MPS recognises that the statutory powers governing the acquisition, retention, use and disclosure of photographs do not, of themselves, determine the lawfulness of subsequent biometric processing using OIFR. The acquisition and retention of a photograph, and the subsequent use of facial recognition technology in relation to that photograph, are distinct activities which each require a lawful basis. The MPS considers that the lawful acquisition and retention of photographs pursuant to statutory powers provides the basis upon which such images may lawfully be held by the MPS. The subsequent biometric processing undertaken through OIFR is justified by the exercise of policing functions recognised at common law, including the prevention and detection of crime, the investigation of offences, the safeguarding of vulnerable persons and the protection of life and public safety. Such processing must additionally comply with the requirements of Part 3 of the Data Protection Act 2018, the Human Rights Act 1998, the Equality Act 2010, relevant codes of practice and the safeguards contained within the OIFR Policy Documents. The fact that an image may lawfully be held by the MPS does not, without more, authorise an OIFR Search.

Other statutory powers

4.23. In addition to PACE, a number of statutory schemes provide powers to photograph and identify individuals in specified circumstances. Where photographs are lawfully obtained pursuant to such powers, they may subsequently be used as Probe Images for OIFR Searching, provided that the use of OIFR falls within a Permitted Use Case and complies with the OIFR Policy, this Legal Mandate and the wider legal framework.

(i) **Terrorism Act 2000**: Paragraph 2 of Schedule 8 empowers authorised persons to take steps reasonably necessary to photograph, measure or otherwise identify detained persons.

(ii) **Counter-Terrorism and Border Security Act 2019**: Paragraph 26 of Schedule 3 provides powers to photograph individuals subject to examination under that Schedule.

(iii) **National Security Act 2023**: Paragraph 2 of Schedule 6 permits authorised persons to take reasonable steps to photograph, measure or otherwise identify detained persons.

(iv) **Immigration Act 1971**: Paragraph 18 of Schedule 2 permits a constable to take steps reasonably necessary to photograph, measure or otherwise identify a detained individual.

Common law powers to acquire, retain and use Probe Images

4.24. Where no specific statutory power is relied upon, the MPS may rely upon common law policing powers to acquire, retain and use photographs for legitimate policing purposes.

4.25. The courts have repeatedly recognised the existence of such powers. In *Wood v Commissioner of Police of the Metropolis*[1], the Court of Appeal confirmed that the police may lawfully take and retain photographs pursuant to common law powers. In *Catt v Association of Chief Police Officers*[2], the Supreme Court recognised that the police may collect and retain information for policing purposes, subject to appropriate safeguards. In *Hellewell v Chief Constable of Derbyshire*[3], the court recognised that photographs may be used for the prevention and detection of crime, the investigation of offences and the apprehension of offenders. In Bridges, the Court of Appeal further recognised that the police possess common law powers to take photographs of individuals in public places.

4.26. Taken together, these authorities support the proposition that the police may lawfully acquire, retain and use photographs pursuant to common law powers for legitimate policing purposes, including the prevention and detection of crime, the investigation of offences, the identification of individuals and the apprehension of offenders.

4.27. Where photographs are lawfully obtained pursuant to common law powers, they may subsequently be used as Probe Images within OIFR, provided that the proposed OIFR Search falls within a Permitted Use Case and complies with the OIFR Policy, this Legal Mandate and the wider legal framework governing biometric processing.

Lawful Possession of Images and OIFR Searching

4.28. Any Probe Image or image contained within a Permitted Image Reference Library must be lawfully held by the MPS and subject to appropriate governance, retention and review arrangements.

4.29. The lawful acquisition, retention or possession of an image does not, of itself, authorise its use for OIFR. Before an OIFR Search may be conducted, the decision-maker must be satisfied that the proposed search falls within a Permitted Use Case, concerns a Permitted Probe Subject, utilises a lawfully acquired Probe Image and an authorised Permitted Image Reference Library, is necessary and proportionate, and complies with the safeguards contained within the OIFR Policy Documents.

4.30. The distinction between the lawful possession of an image and its subsequent use for biometric processing is a fundamental safeguard within the OIFR framework.

[1] [2009] EWCA Civ 414
[2] [2012] EWHC 1471 (Admin)
[3] [1995] 1 WLR 804

5. MPS OIFR Policy

5.1. The MPS has developed the OIFR Policy to ensure that the use of OIFR is lawful, necessary and proportionate, and reflects the principles governing the use of facial recognition technology identified in recent jurisprudence. The Policy is intended to support compliance with the MPS's obligations under the:

(i) Human Rights Act 1998;

(ii) Equality Act 2010;

(iii) Data Protection Act 2018;

(iv) Protection of Freedoms Act 2012; and

(v) Freedom of Information Act 2000.

6. Human Rights Act 1998

Article 8 European Convention of Human Rights ('ECHR')

6.1. The use of OIFR engages Article 8 ECHR because it involves the processing of biometric data. The MPS considers that OIFR is capable of being used compatibly with Article 8 where its use:

(i) pursues a legitimate aim;

(ii) is in accordance with the law;

(iii) is necessary in a democratic society; and

(iv) is proportionate to the policing objective being pursued.

6.2. Whether a particular use of OIFR is necessary and proportionate will depend upon the circumstances of the case and the safeguards contained within the OIFR Policy documents.

In accordance with law

6.3. Any interference with Article 8 rights arising from the use of OIFR must be in accordance with the law. This requires the legal framework governing OIFR to be sufficiently accessible and foreseeable and to contain adequate safeguards against arbitrary or disproportionate use.

6.4. In *Bridges*, the Court of Appeal confirmed that the use of facial recognition technology must be governed by a legal framework which provides sufficient guidance as to the circumstances in which the technology may be used and the limits on the exercise of police discretion.

6.5. The MPS considers that the use of OIFR satisfies these requirements through the combined effect of common law policing powers, statutory powers, the Human Rights Act 1998, the Data Protection Act 2018, equality legislation and the OIFR Policy Documents. Together, these provisions define the circumstances in which OIFR may be used, the

persons who may be subject to an OIFR Search, the images that may be used as Probe Images or within Permitted Image Reference Libraries, and the safeguards, governance and oversight arrangements applicable to its use.

Accessibility

6.6. The requirement of accessibility is intended to ensure that the legal framework governing OIFR is sufficiently available and understandable to those affected by its use.

6.7. The MPS seeks to satisfy this requirement through the publication of the OIFR Policy Documents and associated transparency materials. These documents describe the purposes for which OIFR may be used, the legal powers relied upon by the MPS, the categories of images that may be searched, the circumstances in which OIFR Searches may be conducted, and the safeguards governing the use of the technology.

6.8. In particular, the OIFR framework prescribes the Permitted Use Cases for which OIFR may be deployed, the categories of Permitted Probe Subject, the requirements applicable to Probe Images and Permitted Image Reference Libraries, and the approval, audit, retention, review and oversight arrangements that apply to OIFR Searches. The MPS considers that these measures provide a sufficiently accessible framework governing the use of OIFR.

Foreseeability

6.9. The use of OIFR must be governed by sufficiently clear and predictable rules so that its application is not dependent upon the unfettered discretion of individual decision-makers.

6.10. As recognised in *Bridges* (and subsequently applied in *R (Thompson and Carlo) v Commissioner of Police of the Metropolis*[4]), foreseeability does not require an inflexible regime. It does, however, require safeguards which sufficiently constrain operational discretion and protect against arbitrary interference with Convention rights.

6.11. The MPS considers that the OIFR Policy addresses those requirements by identifying the purposes for which OIFR may be used, the categories of subjects, images and databases that may be searched, and the safeguards governing the conduct and oversight of OIFR Searches.

6.12. In broad terms, the OIFR Policy addresses foreseeability through three questions:

(i) the "Why Question" - why OIFR may be used;

(ii) the "What Question" - what subjects, images and databases may be searched; and

(iii) the "How Question" - how OIFR Searches may be conducted and governed.

The "Why Question"

6.13. The OIFR Policy addresses the "Why Question" by restricting the use of OIFR to defined policing purposes and specified Permitted Use Cases.

[4] [2026] EWHC 915 (Admin)

6.14. OIFR may only be used where it supports a legitimate policing objective and where its use has been assessed as necessary and proportionate in all the circumstances.

The "What Question"

6.15. The OIFR Policy addresses the "What Question" by defining:

(i) the categories of Subject who may be searched;

(ii) the categories of Probe Image which may be used;

(iii) the Image Matrix used to assess privacy considerations and determine approval requirements;

(iv) additional safeguards applicable in circumstances involving protected characteristics or heightened privacy considerations; and

(v) the Permitted Image Reference Libraries against which searches may be conducted.

6.16. The Policy also contains requirements relating to the retention, review and dissemination of Probe Images and OIFR results.

6.17. Taken together, these provisions place clear limits on the persons, images and databases that may be used for OIFR purposes.

The "How Question"

6.18. The OIFR Policy addresses the "How Question" by prescribing the circumstances in which OIFR may be used and the safeguards governing its operation.

6.19. Those safeguards include:

(i) requirements relating to necessity and proportionality;

(ii) approval and escalation processes in defined circumstances;

(iii) technical safeguards intended to minimise unnecessary biometric processing;

(iv) mandatory human review of OIFR results;

(v) transparency requirements; and

(vi) governance, audit and oversight arrangements.

6.20. Taken together, these measures provide a structured framework governing the use of OIFR and are intended to ensure that OIFR is exercised in a foreseeable, transparent and accountable manner.

Legitimate Aim

6.21. Article 8 recognises, amongst other matters, the prevention and detection of crime, public safety and the protection of the rights and freedoms of others as legitimate aims.

6.22. The use of OIFR in accordance with the OIFR Policy is capable of advancing those legitimate aims.

6.23. An OIFR User may only use OIFR for the specific operational purposes set out in the OIFR Policy, namely: (a) supporting the identification of a subject for a law enforcement purpose; and (b) ascertaining whether an arrested or otherwise detained person poses a risk to themselves or others. These use cases support the prevention and detection of crime, public safety, safeguarding activity and the protection of the rights and freedoms of others.

Necessity and Proportionality

6.24. The MPS recognises that necessity and proportionality are fact-sensitive assessments that must be considered in every deployment. In assessing the necessity and proportionality of an OIFR Search, regard should be had to all relevant circumstances, including the nature and provenance of the Probe Image, the purpose of the proposed search, the image repositories to be searched, and the individual's reasonable expectation of privacy. The degree of interference with Article 8 rights may vary depending upon factors including whether an image was obtained in a public or private setting, whether it was obtained pursuant to a statutory power or common law policing function, the original purpose for which it was obtained, and whether it reveals information about an individual's private life. These considerations are reflected in the OIFR Policy, including the Image Matrix, approval requirements and the specific safeguards applicable to each OIFR use case

6.25. The necessity and proportionality assessment applicable to Use Case B must be considered in light of the particular circumstances of detention and the statutory powers under which the Probe Image was obtained. Regard must be had to the operational purpose of the proposed OIFR Search, including whether the search is necessary to assist in establishing identity or identifying information relevant to the safe, lawful and effective management of the detained person. The MPS OIFR Policy sets out the specific proportionality considerations, safeguards and approval requirements applicable to Use Case B and must be complied with in every case.

6.26. The OIFR Policy adopts a range of safeguards designed to ensure any use of OIFR is targeted, justified and proportionate to the legitimate aim pursued. These include restrictions on the categories of persons who may be searched, limitations upon the image datasets that may be searched, approval requirements, audit requirements and retention controls.

6.27. Accordingly, the MPS considers that the use of OIFR in accordance with the OIFR Legal Framework is capable of being compatible with Article 8 ECHR.

Transparency

6.28. Transparency forms an important safeguard within the OIFR framework. The OIFR Policy contains requirements concerning notification of subjects, the provision of information regarding OIFR use, additional safeguards in circumstances involving heightened privacy expectations, and the use of body-worn video where appropriate.

Article 9 ECHR

6.29. The use of OIFR may engage an individual's rights under Article 9 ECHR, which protects freedom of thought, conscience and religion. Article 9 protects both the right to hold religious or other beliefs and the right to manifest those beliefs, whether alone or in

community with others, in public or in private, through worship, teaching, practice and observance. The law provides:

"Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in worship, teaching practice and observance. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

6.30. Article 9 may become relevant where a Probe Image depicts a person wearing items of religious clothing, attending a place of worship, participating in a religious event or ceremony, or otherwise manifesting a religious or philosophical belief. In such circumstances, decision-makers must have regard to whether the proposed use of OIFR could have a chilling effect on an individual's willingness to manifest their beliefs or participate in religious activities.

6.31. As Article 9 is a qualified right, any interference with that right will only be lawful where:

(i) the interference is in accordance with the law and has a sufficiently clear legal basis;

(ii) the use of OIFR pursues a legitimate aim (as set out in Section 1 of this Legal Mandate);

(iii) the interference is necessary in a democratic society; and

(iv) the use of OIFR is proportionate to the legitimate aim pursued.

6.32. Where Article 9 considerations arise, they should form part of the proportionality assessment undertaken in accordance with the OIFR Policy. Particular care should be taken where the Probe Image was obtained at or near a place of worship, during a religious gathering, or in other circumstances where the use of OIFR may affect the exercise of Convention rights

Articles 10 and 11 ECHR

6.33. The use of OIFR may, in certain circumstances, engage rights protected by Articles 10 and 11 ECHR. These rights may be particularly relevant where a Probe Image has been obtained in the context of a protest, demonstration, public assembly, political gathering, campaign event, or other activity involving the exercise of rights to freedom of expression, peaceful assembly, or association.

6.34. Article 10 protects the right to hold opinions and to receive and impart information and ideas without interference by public authority. Article 11 protects the right to peaceful assembly and freedom of association with others. These rights are closely connected and will often arise together. The law provides:

Article 10: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Article 11: "Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the state."

6.35. As qualified rights, any interference with an individual's Article 10 and/or Article 11 rights will only be lawful where:

(i) the interference is in accordance with the law and has a sufficiently clear legal basis;

(ii) the use of OIFR pursues a legitimate aim;

(iii) the interference is necessary in a democratic society; and

(iv) the use of OIFR is proportionate to the legitimate aim pursued.

6.36. Particular care should be taken where a Probe Image was obtained during, or in connection with, the exercise of rights protected by Articles 10 and 11. In such circumstances, OIFR Users and decision-makers must consider whether the proposed use of OIFR could have a chilling effect on an individual's willingness, to exercise their rights to freedom of expression, peaceful assembly, or association. These considerations should form part of the proportionality assessment undertaken before an OIFR Search is conducted.

Article 14 ECHR

6.37. Article 14 requires that the rights and freedoms protected by the ECHR are secured without discrimination. The principle underpinning Article 14 is that all individuals should be able to enjoy Convention rights equally, regardless of their personal characteristics. The law provides:

"The enjoyment of the rights and freedoms set forth in the European Convention on Human Rights and the Human Rights Act shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

6.38. Article 14 is not a free-standing right and may only be relied upon in conjunction with another Convention right. It may be engaged where the exercise or enjoyment of another Convention right is affected by differential treatment on the basis of a protected characteristic or other status. In the context of OIFR, consideration should therefore be given to whether the selection or use of a Probe Image, the conduct of an OIFR Search, or any related operational decision-making could have a disproportionate or discriminatory impact on individuals or groups sharing a particular protected characteristic.

6.39. Decision-makers must have regard to the possibility of direct or indirect discrimination and ensure that decisions relating to the use of OIFR are based on objective, lawful and proportionate grounds. Particular consideration should be given to whether the proposed use of OIFR could result in a disproportionate impact on individuals sharing a protected characteristic.

6.40. These considerations are supported by the OIFR Equality Impact Assessment and the safeguards contained within the OIFR Policy, including the Probe Image Levels Framework, enhanced authorisation requirements, protected characteristic considerations and audit and oversight mechanisms. Where Article 14 considerations arise, they should form part of the proportionality assessment and be recorded within the OIFR Submission Form to demonstrate that equality impacts have been expressly considered before an OIFR Search is authorised.

Operational Duties

6.41. In addition to respecting Convention rights, the MPS is subject to positive obligations under Articles 2 and 3 of the ECHR. Article 2 protects the right to life and Article 3 protects individuals from torture and inhuman or degrading treatment. Both are absolute rights and cannot be limited or qualified.

6.42. Articles 2 and 3 may require the police to take reasonable and proportionate operational measures where there is a known, or reasonably foreseeable, risk to life or risk of serious harm. In certain circumstances, those positive obligations may be relevant when considering the use of OIFR as an investigative or safeguarding tool.

6.43. In *Osman v United Kingdom* (1998) 29 EHRR 245, the European Court of Human Rights recognised that public authorities may be required to take reasonable measures to protect an identified individual, or individuals, from a real and immediate risk to life of which the authorities knew or ought reasonably to have known. Article 3 may similarly give rise to positive obligations to take reasonable steps to prevent, investigate and respond to a credible risk of torture, inhuman treatment or degrading treatment.

6.44. These operational duties are most likely to be relevant to the use of OIFR in circumstances where:

(i) the timely identification of a person may assist in addressing a real and immediate risk to life or a credible risk of serious harm;

(ii) an OIFR Search is capable of advancing an urgent safeguarding, missing person or public protection investigation; or

(iii) following the generation and adjudication of a Potential OIFR Match, prompt operational action may be required to protect an individual or the public from harm.

6.45. Where Articles 2 or 3 are engaged, the existence of a real and immediate risk to life, or a credible risk of serious harm, may be a significant factor in assessing the necessity and proportionality of an OIFR Search. However, the use of OIFR must remain lawful, necessary and proportionate in accordance with this Legal Mandate and the OIFR Policy.

7. Equality Act 2010

7.1. The MPS is subject to the Public Sector Equality Duty ("PSED") under section 149 of the Equality Act 2010. In exercising its functions, the MPS must have due regard to the need to:

(i) Eliminate unlawful discrimination, harassment and victimisation;

(ii) Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and

(iii) Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

7.2. The MPS recognises that the use of OIFR has the potential to affect individuals who possess protected characteristics under the Equality Act 2010. Particular consideration has therefore been given to whether the deployment and operation of OIFR could result in direct or indirect discrimination, unequal treatment, or disproportionate impacts upon particular groups.

7.3. In developing the OIFR Policy and associated governance framework, the MPS has considered equality impacts through the completion of an Equality Impact Assessment and through consultation with relevant stakeholders. The MPS will continue to keep equality impacts under review as OIFR develops and operational practice evolves.

7.4. The MPS recognises that, as with any policing tactic involving the processing of personal information, public confidence depends upon ensuring that OIFR is used fairly, lawfully and consistently. OIFR must not be used on the basis of assumptions, stereotypes or generalisations relating to protected characteristics.

7.5. Equality considerations are reflected throughout the OIFR Policy. In particular, the Policy places restrictions on the circumstances in which OIFR may be used, identifies permitted operational use cases, limits the categories of person who may be the subject of a search and requires decision-makers to consider necessity, proportionality and the potential impact upon affected individuals before authorising use.

7.6. Additional safeguards are incorporated within the OIFR Policy where the proposed use of OIFR may involve individuals whose circumstances require particular consideration. Annex D sets out enhanced governance measures applicable in specified cases, including additional scrutiny, authorisation requirements, restrictions on use, retention controls and requirements to seek specialist advice. These provisions include safeguards relating

to children, persons with relevant disabilities and circumstances involving gender reassignment, and are intended to reduce the risk of unjustified or disproportionate impacts on individuals with protected characteristics or other vulnerable groups.

7.7. The MPS also recognises that accuracy and performance are important equality considerations where facial comparison technologies are used. The MPS therefore requires OIFR systems to undergo appropriate testing, evaluation and assurance processes. Human review remains an integral element of operational decision-making and no person will be subject to police action solely on the basis of an OIFR system output.

7.8. Compliance with the Equality Act 2010 is not a one-off assessment. Equality considerations form part of the ongoing governance and oversight arrangements applicable to OIFR deployments. Operational use, performance data, audit information and equality impacts will be monitored and reviewed to ensure that OIFR continues to operate in a manner that is lawful, necessary, proportionate and consistent with the Public Sector Equality Duty.

8. Data Protection Act 2018

Law Enforcement Processing

8.1. The processing of personal data through OIFR is undertaken pursuant to Part 3 of the Data Protection Act 2018 ("DPA 2018"). The MPS may only process personal data using OIFR where the processing is for a law enforcement purpose within the meaning of section 31 DPA 2018, namely: *"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."*

8.2. The OIFR Policy restricts the use of OIFR to defined and approved use cases to ensure that all OIFR processing is undertaken for a lawful law enforcement purpose.

Sensitive Processing

8.3. OIFR involves the processing of biometric data for the purpose of uniquely identifying individuals and therefore constitutes sensitive processing under section 35 DPA 2018. Accordingly, OIFR may only be used where:

(i) the processing is strictly necessary for the relevant law enforcement purpose;

(ii) the processing satisfies a Schedule 8 condition; and

(iii) an Appropriate Policy Document is in place.

8.4. In this context, "strictly necessary" requires decision-makers to be satisfied that there is a pressing policing need for the processing and that the objective cannot reasonably be achieved by less intrusive means. Relevant considerations may include:

(i) the nature and seriousness of the policing purpose being pursued;

(ii) whether alternative investigatory or identification methods have been considered and discounted;

(iii) the anticipated benefits of the proposed OIFR Search;

(iv) the nature of the Probe Image and proposed Image Reference Library; and

(v) whether the intrusion arising from the processing is justified by the policing objective being pursued.

8.5. These considerations form part of the necessity and proportionality assessment required by the OIFR Policy.

Schedule 8 Condition

8.6. The MPS relies upon paragraph 1 of Schedule 8 DPA 2018, namely that the processing is:

(i) necessary for the exercise of a function conferred by an enactment or rule of law; and
(ii) necessary for reasons of substantial public interest.

8.7. The specific policing purpose supporting an OIFR Search, together with the necessity and proportionality assessment, must be recorded through the OIFR authorisation process.

Data Protection Impact Assessment

8.8. The MPS has undertaken a Data Protection Impact Assessment ("DPIA") in relation to the use of OIFR. The DPIA identifies the risks to the rights and freedoms of data subjects arising from OIFR and the safeguards implemented to mitigate those risks.

8.9. These safeguards include controls relating to purpose limitation, lawful use cases, authorisation requirements, necessity and proportionality assessments, equality impacts, protected characteristics, human adjudication, retention and deletion requirements, governance, audit, system assurance and information security.

8.10. The DPIA is a living document and will be kept under review alongside the OIFR Policy, Appropriate Policy Document and associated governance arrangements.

Data Protection by design

8.11. Part 3 DPA 2018 requires the MPS to implement appropriate technical and organisational measures designed to integrate data protection into processing activities. OIFR has therefore been designed and governed to support compliance with the law enforcement data protection principles, including requirements relating to lawfulness, fairness, purpose limitation, data minimisation, accuracy, retention and security.

8.12. The safeguards implemented through the OIFR Policy, DPIA, Appropriate Policy Document and associated governance documentation include measures relating to:

(i) the acquisition, assessment and use of Probe Images;

(ii) the creation and use of approved Image Reference Libraries;

(iii) defined use cases and authorisation requirements;

(iv) necessity and proportionality assessments;

(v) mandatory human review and adjudication of Potential OIFR Matches;

(vi) equality and protected characteristic considerations;

(vii) audit, governance and oversight arrangements;

(viii) retention, review and deletion requirements;

(ix) OIFR user training;

(x) technical assurance and ongoing monitoring of system performance; and

(xi) technical and organisational security controls governing access, storage, transmission and deletion of data.

8.13. The detail of these safeguards is set out within the OIFR Policy, DPIA and Appropriate Policy Document, which should be read alongside this Legal Mandate.

Appropriate Policy Document

8.14. Section 42 DPA 2018 requires an Appropriate Policy Document to be in place when undertaking sensitive processing for law enforcement purposes. The MPS has produced and published an Appropriate Policy Document which explains:

(i) the categories of personal data processed through OIFR;
(ii) the procedures and safeguards used to ensure compliance with the law enforcement data protection principles;
(iii) the accountability measures applicable to OIFR processing; and
(iv) the retention and erasure arrangements governing OIFR processing.

Data Protection Officer

8.15. The MPS has appointed a Data Protection Officer in accordance with Part 3 DPA 2018. The Data Protection Officer provides advice and oversight regarding compliance with data protection obligations, including those relating to OIFR, and forms part of the wider governance and assurance framework applicable to the use of OIFR.

Ongoing compliance and review

8.16. Compliance with the DPA 2018 is an ongoing obligation. The use of OIFR will therefore remain subject to audit, governance, oversight and periodic review to ensure that the processing of personal data remains lawful, necessary, proportionate and consistent with the safeguards set out in the OIFR Policy, DPIA and Appropriate Policy Document.

9. Legal Considerations Regarding Using OIFR in relation to the Deceased

9.1. The use of OIFR to assist in the identification of a deceased person gives rise to a number of distinct legal and ethical considerations.

Data Protection

9.2. The Data Protection Act 2018 applies to information relating to identified or identifiable living individuals. Accordingly, information relating solely to a deceased person does not constitute personal data for the purposes of the Data Protection Act 2018. However, OIFR searches undertaken to identify a deceased person may involve the processing of personal data relating to living individuals, including family members, witnesses or other persons connected to the investigation. Such processing must therefore continue to comply with the requirements of the Data Protection Act 2018, the OIFR Policy, the DPIA and the Appropriate Policy Document.

9.3. Whilst information relating solely to a deceased person falls outside the scope of data protection legislation, users should nonetheless continue to act lawfully, respectfully and with appropriate regard to any confidentiality considerations and the potential impact on surviving relatives.

Human Rights considerations

9.4. Although Convention rights do not generally continue after death, Article 8 ECHR may remain relevant in relation to the rights and interests of surviving family members.

9.5. In *Lozovyye v Russia*, the European Court of Human Rights recognised that issues surrounding the treatment of a deceased person, including the notification of family members and arrangements following death, may engage the Article 8 rights of surviving relatives. The Court emphasised the importance of enabling family members to obtain information concerning the death of a relative and to participate in matters relating to burial and remembrance. In this respect, the timely identification of deceased persons may assist the MPS in informing next of kin and supporting bereaved families.

9.6. Similarly, in *Putistin v Ukraine,* the Court recognised that Article 8 may extend to the protection of a deceased person's memory and reputation where this has a direct impact upon surviving relatives. Whilst the case concerned reputational issues, it demonstrates that the treatment of deceased persons may continue to engage the rights and interests of living family members.

Dignity and respect

9.7. Where OIFR is used to assist in the identification of a deceased person, users should have regard to the potential impact on surviving relatives and ensure that the process is conducted with dignity, sensitivity and respect.

9.8. In appropriate circumstances, OIFR may provide a less intrusive means of assisting identification than alternative methods and may support the MPS in discharging its wider investigatory, safeguarding and family liaison functions. The use of OIFR must nevertheless remain lawful, necessary and proportionate in accordance with the requirements of the OIFR Policy.

10. Freedom of Information Act 2000

10.1. The Freedom of Information Act 2000 ("FOIA") provides a framework through which the public may obtain access to information held by public authorities. FOIA promotes transparency and accountability by:

(i) requiring public authorities to make certain information routinely available; and
(ii) providing a right for members of the public to request access to recorded information held by public authorities.

10.2. In recognition of these obligations, the MPS seeks to ensure an appropriate degree of transparency regarding its use of OIFR. This includes the publication of information concerning the legal, ethical and governance framework supporting OIFR, including relevant policy documents, impact assessments and other supporting material where appropriate.

10.3. The MPS will consider and respond to FOIA requests concerning OIFR in accordance with the requirements of the Act. Any disclosure will be subject to the exemptions contained within FOIA and to the MPS's wider legal obligations, including those relating to law enforcement, national security, personal data and information security.

10.4. Transparency is an important safeguard supporting public confidence in the use of OIFR. The publication of information relating to OIFR, together with appropriate governance, oversight and reporting arrangements, assists in ensuring that the use of OIFR remains lawful, accountable and subject to public scrutiny.

11. Impact Assessments

11.1. Consistent with the requirements of the OIFR Policy and relevant statutory obligations, the MPS has undertaken a number of impact assessments in relation to the use of OIFR. These assessments are designed to identify, assess and mitigate potential risks arising from the use of OIFR and to ensure that appropriate safeguards are implemented.

11.2. The principal impact assessments supporting the use of OIFR are:

(i) the Data Protection Impact Assessment ("DPIA"), which considers the impact of OIFR on the rights and freedoms of data subjects and identifies the measures implemented to ensure compliance with the Data Protection Act 2018; and
(ii) the Equality Impact Assessment ("EIA"), which considers the potential equality impacts arising from the use of OIFR and identifies the safeguards implemented to support compliance with the Equality Act 2010 and the Public Sector Equality Duty.

11.3. The findings and recommendations arising from these assessments have informed the development of the OIFR Policy, associated governance arrangements, operational safeguards and approval processes. The assessments should therefore be read alongside this Legal Mandate and the OIFR Policy as part of the wider framework governing the use of OIFR.

11.4. The DPIA and EIA are living documents and will be kept under review to ensure that they continue to accurately assess risks and reflect any relevant legal, operational, technical or policy developments relating to OIFR.

11.5. The impact assessments conclude that, when OIFR is used in accordance with the OIFR Policy, associated governance arrangements and identified safeguards, the use of OIFR is capable of being operated in a manner that is consistent with the MPS's legal obligations.