# EQUALITY IMPACT ASSESSMENT
# STEPS 1 TO 7

## STEP 1. Aims and purpose of the proposal / policy

GUIDANCE

### THE PURPOSE OF OPERATOR INITIATED FACIAL RECOGNITION (OIFR)

OIFR is a digital policing capability that enables the MPS to compare a lawfully obtained image of an individual against Permitted Image Reference Libraries to support identification for a policing purpose. OIFR may assist officers and staff where identification is necessary for a law enforcement purpose or to ascertain whether an arrested or otherwise detained person poses a risk to themselves or others. OIFR is deployed only where it is lawful, necessary, proportionate, and in pursuit of a legitimate policing aim.

The MPS may only use OIFR in accordance with the specific use cases set out within Section 2 of the MPS OIFR Policy and associated governance documents.

### BENEFITS OF OIFR

The MPS has drawn extensively upon its operational experience of using Live Facial Recognition (LFR) and Retrospective Facial Recognition (RFR) to inform the development and deployment of OIFR. The MPS considers OIFR to be a valuable policing capability which complements a wider range of tools and systems already used within policing to prevent and detect crime, safeguard vulnerable individuals and protect the public. These tools include, but are not limited to, the Police National Database (PND), Automated Number Plate Recognition (ANPR), Closed-Circuit Television (CCTV) and Body-Worn Video (BWV).

OIFR enables authorised users to compare an image against Permitted Image Reference Libraries in circumstances where identification is necessary for a permitted policing purpose. By assisting officers and staff in progressing identification enquiries, OIFR can support the prevention and detection of crime, the safeguarding of vulnerable people, public protection, and the effective management of policing operations.

OIFR may assist officers and investigators to:

- develop investigative or intelligence leads where identification would otherwise remain unresolved or require more resource-intensive or intrusive enquiries;
- support identification where alternative methods, such as biographical checks or fingerprints, are unavailable, inconclusive or impracticable in the circumstances;
- support timely operational decision-making where a prompt understanding of an individual's identity is relevant to a lawful policing objective;
- support less intrusive policing outcomes by reducing the need for arrest, detention or the collection of additional biometric information where identification can be sufficiently progressed through OIFR and alternative legal powers are not required; and
- reduce reliance on manual and time-intensive enquiries that may delay safeguarding activity, investigative progression or operational decision-making.

Any potential match returned by OIFR does not constitute proof of identity and must be subject to human review and assessment alongside all other available information.

**Accelerating MPS investigations and operations**

OIFR may be used by authorised officers and staff where the circumstances fall within a permitted use case and the

relevant legal, policy and governance requirements have been satisfied. This may include situations where the identity of an individual is unknown or reasonably doubted and establishing that identity is necessary for a law enforcement purpose, or where identifying an arrested or detained individual is necessary to assist in assessing risk to themselves or others.

By assisting in establishing identity at an earlier stage, OIFR can support more effective safeguarding, risk management and investigative decision-making. It may also assist officers and staff in prioritising resources and progressing enquiries more efficiently, enabling policing activity to be directed where it is most needed.

Further examples may include:

i. **Locating missing persons** - where officers encounter an individual believed to require safeguarding but who is unwilling or unable to identify themselves, OIFR may assist in progressing identification and enabling appropriate safeguarding measures to be considered at the earliest opportunity.

ii. **Supporting the safeguarding of children and vulnerable persons** - where officers engage with a child or vulnerable individual who may be at risk of harm or exploitation, OIFR may assist in progressing identification to support safeguarding activity.

iii. **Assisting with identification enquiries** - where an individual is unwilling or unable to provide details of their identity, or where there are reasonable grounds to doubt the identity provided, OIFR may assist in progressing identification where this is necessary for a permitted policing purpose.

iv. **Assisting with identifying deceased or incapacitated persons** - where a person is unable to identify themselves due to incapacity, injury or other circumstances, OIFR may assist in progressing identification enquiries in support of safeguarding, investigative or coronial processes.

v. **Supporting risk management within custody and detention settings** - OIFR may assist in establishing the identity of an arrested or detained person where there are reasonable grounds to believe they may be providing false details or concealing their identity. Earlier identification may assist officers and staff in obtaining information relevant to risk assessment, safeguarding and the safety of detainees, officers, staff and others.

**Use to mitigate threats to public safety**

OIFR may support operational policing responses where the identification of individuals is necessary to assist in addressing threats to public safety. This may include circumstances associated with serious incidents, major investigations or critical incidents where establishing an individual's identity is necessary to support an effective policing response.

Where lawful, necessary and proportionate, OIFR may assist officers in progressing identification enquiries more quickly, enabling information to be assessed and acted upon in support of public protection and operational decision-making.

In all circumstances, OIFR shall only be used in accordance with the MPS OIFR Policy, applicable legislation, governance requirements and the safeguards set out within the Data Protection Impact Assessment and associated operational procedures.

**PURPOSE OF THE EQUALITY IMPACT ASSESSMENT (EIA)**

The purpose of this EIA is to assess this proposal for equality impact against staff and service users effected by the proposal's implementation. Conducting this assessment aims to identify disadvantages suffered by any individual and/or group safeguarded by a protected characteristic, and by those who are not (for example, 'socio-economic' groups).

The aim is to mitigate any identified disadvantage by eliminating the impact, reducing the impact or accepting the impact. If elimination and/or reduction is not possible the MPS are required to implement a positive action strategy or provide a justification rationale for not doing so under the criterion of 'Proportionality, Legality, Accountability and Necessity'.

The purpose of conducting EIAs is to meet the legal requirements set out in the 'Public Sector Equality Duty (PSED), and specifically, in relation to the **3 Aims** and **3 Specific Duties** under section 149 of the Equality Act 2010 (the Act).

**The 3 Aims:**

In summary, those subject to the PSED must, in exercising their functions, have due regard to the need to:

- ✓ Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- ✓ Advance equality of opportunity between people who share a protected characteristic and those who do not.
- ✓ Foster good relations between people who share a protected characteristic and those who do not.

**The Three Specific Duties:**

The Act explains that having due regard for advancing equality involves:

- ✓ Removing or minimising disadvantages suffered by people due to their protected characteristics.
- ✓ Taking steps to meet the needs of people from protected groups where these are different from the needs of other people.
- ✓ Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

This EIA concerns the use of OIFR by the MPS in principle, in accordance with the MPS OIFR Policy, rather than any specific authorisation of an Image Reference Library and OIFR Search. However, the MPS recognises that the Public Sector Equality Duty is an ongoing duty. To the extent that an Image Reference Library or OIFR Search raises specific equality considerations, these must be considered by the relevant decision maker in accordance with Section 6 of the Policy.

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

| STEP 2. Screening process for relevance to diversity and equality issues | | | | GUIDANCE |
|---|---|---|---|---|
| Each 'protected characteristic' in Section 5 has guidance as to what implications / issues you may need to consider. | | | | |
| Does this proposal / policy have any relevance to: | | Internal, relevant to staff / or working practices | External, relevant to service delivery | Not relevant to either |
| A | Age | ☐ Yes | ☒ Yes | ☐ Yes |
| B | Deaf and disabled / Disability | ☒ Yes | ☒ Yes | ☐ Yes |
| C | Gender Reassignment | ☐ Yes | ☒ Yes | ☐ Yes |
| D | Marriage and Civil Partnership (employment only) | ☐ Yes | ☐ Yes | ☒ Yes |
| E | Pregnancy and Maternity | ☐ Yes | ☐ Yes | ☒ Yes |
| F | Race | ☐ Yes | ☒ Yes | ☐ Yes |
| G | Religion or Belief | ☒ Yes | ☒ Yes | ☐ Yes |
| H | Sex | ☐ Yes | ☒ Yes | ☐ Yes |
| I | Sexual Orientation | ☐ Yes | ☐ Yes | ☒ Yes |
| J | Other Issues | ☐ Yes | ☒ Yes | ☐ Yes |

| STEP 3. If you have ticked yes to any protected characteristic box in Step 3, a full impact assessment is required. | | GUIDANCE |
|---|---|---|
| Full assessment required? (If Yes, a full EIA is required.) | ☒ Yes | ☐ No |

## P 4. Examination of available information

**Legal Framework - section 149 of the Equality Act 2010 (the Act) – Public Sector Equality Duty (PSED)**

***http://www.legislation.gov.uk/ukpga/2010/15/contents***

Section 149 of the Act sets out legal obligations for Public Sector Organisations known as the Public Sector Equality Duty.

**Equality & Human Rights Commission - Public Sector Equality Duty – Technical Guidance**

**Meeting the Equality Duty in Policy and Decision Making**

Key Learning Points:

- ✓ Impacted groups to consider include Internal Staff and External Service Users.
- ✓ The impact of protected characteristics individuals or groups within the above two categories.
- ✓ The analysis of diversity data/protected characteristics information on staff and service users affected the proposal.
- ✓ Requirement to make 'evidence-based' decisions.
- ✓ Data gathered must be quantitative and qualitative, based on current, accurate data sources.
- ✓ If data is unavailable the relevant body must demonstrate due regard in order to obtain it.

The Technical Guidance lists key Discriminatory Exceptions:

> *The basic presumption under the Act is that discrimination because of a protected characteristic in unlawful. However, the act recognises that not all people can be treated the same, and people with different protected characteristics can be treated differently to reflect their particular needs. The Act recognises that compliance with the duty may involve treating some people more favourably than others.*

The Act achieves this in three main ways:

- ✓ By requiring people with some protected characteristics to be treated differently (e.g. making reasonable adjustments for disabled people)

- ✓ By setting out exceptions to the application of the Act's provisions, which apply to a specific protected characteristic in certain situations (e.g. allowing same-sex services in some situations)

- ✓ Allowing positive action in limited circumstances (e.g. implementing a 'trigger' policy for people with specific needs, under those specific circumstances)

The law requires that public authorities demonstrate they have had 'due regard' to the aims of the equality duty in their decision-making. Assessing the potential impact on equality of proposed changes to policies, procedures and practices is one of the key ways in which public authorities can demonstrate that they have had 'due regard'. Due regard is demonstrated by the completion of this EIA.

## Equality & Human Rights Commission Guidance - Employment Statutory Codes of Practice

The Statutory Code of Practice provides further guidance on 'Positive Action':

- ✓ Any measures taken to help to alleviate any disadvantage experienced

- ✓ Justification must meet one or more of the 3 Aims / the 3 Specific Duties

- ✓ Decision making must be based on quantifiable evidence

- ✓ Positive action is not the same as positive discrimination, which is unlawful

- ✓ Positive action without continued justification may be deemed unlawful

Organisations need to consider:

- ✓ Is the action an appropriate way to achieve the stated aim?

- ✓ If so, is the proposed action reasonably necessary to achieve the aim?

- ✓ In all of the circumstances, would it be possible to achieve the aim as effectively by other actions that are less likely to result in less favourable treatment of others?

- ✓ Is the action proportionate, legal, accountable and necessary 'P.L.A.N'?

## Equality and Human Rights Commission – Religion or Belief: a guide to the law

'Religion or belief: a guide to the law' provides an overview of the protections offered by the Equality Act 2010 and the Human Rights Act 1998 of people with or without a religion or belief. It answers commonly asked questions such as what is indirect discrimination and can it ever be justified, and how much employers are expected to know about religion or belief.

**Equality and Human Rights Commission – Legal Framework regarding Protected Characteristics:**

https://www.equalityhumanrights.com/en/equality-act/protected-characteristics#age

https://www.equalityhumanrights.com/en/equality-act/protected-characteristics#disability

https://www.equalityhumanrights.com/en/equality-act/protected-characteristics#reassignment

https://www.equalityhumanrights.com/en/equality-act/protected-characteristics#sex

**MPS OIFR Policy Document**

Details the current position of the MPS use of Facial Recognition Technologies. Contains descriptions of the technologies along with a number of additional documents that outline how and when the MPS will use them, impact documents, scientific testing outcomes and results of usage.

Direction for the MPS use of OIFR to identify individuals or determine whether relevant imagery exists to supporting the identification of a subject for a law enforcement purposes and to ascertain if an arrested or otherwise detained person poses a risk to themselves or others. Its use can support the advancement of investigations, the identification of unknown subjects, and other operational activities undertaken to protect the public.

Access via: Live Facial Recognition | Metropolitan Police

**MPS OIFR Legal Mandate**

The Legal Mandate outlines the legal basis for the MPS's use of OIFR technology.

**MPS OIFR Data Protection Impact Assessment (DPIA)**

The DPIA:

- ✓ Describes the nature, scope, context and purposes of the processing;
- ✓ Assesses the necessity, proportionality and compliance measures;
- ✓ Identifies and assesses risks to individuals; and
- ✓ Identifies any additional measures to mitigate those risks.

## OIFR Training Material

The training material will provide mandatory training for the OIFR Users, depending on the role which the User is undertaking. The documents embed the controls and safeguards adopted for the lawful use of OIFR including points around the management of expectations of privacy in relation to certain protected characteristics, and the identification of facial features/identifying features.

**National Physical Laboratory - Facial Recognition Equitability Study**

Explains how to understand OIFR system accuracy and explains what the MPS have done to understand its algorithm and how it does so within an operational context.

**MPS Document: The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences**

Explains how to understand OIFR system accuracy

Explains what the MPS have done to understand its algorithm and how it does so within an operational context.

https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/understanding-accuracy-and- demographic-differences-v3..pdf

**Information available that is relevant to Facial Recognition Technologies:**

Whilst a number of these refer to Live Facial Recognition which has a different application to OIFR, a number of points (such as those relating to the PSED and the assessment of algorithm performance) have relevance to OIFR.

**ICO Report into Police Use of Facial Recognition, October 2019**

https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-

20191031.pdf This report covers a number of points including:

- ✓ Speaking in July 2019, the then Home Secretary, Sajid Javid, said, "I back the police in looking at technology and trialling it and […] different types of facial recognition technology is being trialled especially by the Met at the moment and I think its right they look at that".

- ✓ In January 2019, the ICO commissioned Harris Interactive to conduct market research exploring the public's awareness and perceptions about the police use of LFR in public spaces.

- ✓ A total of 2,202 adults aged 18+ responded to a 10-minute online survey. Separately, 35 adults aged 18+ participated in a one-hour live chat to openly discuss the use of LFR, with certain discussion topics led by a moderator. Results of the online survey were weighted to be nationally representative of the UK by age and gender.

- ✓ In summary: there is strong public support for the use of LFR for law enforcement purposes:
    - 82% of those surveyed indicated that it was acceptable for the police to use LFR;
    - 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;
    - 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime; and
    - 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.

**ICO Guidance on AI and data protection.**
https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

This report covers a number of points including:

- ✓ Accountability principles which makes you responsible for complying with data protection law and for demonstrating that compliance in any AI system that processes personal data.
- ✓ How do the principles of lawfulness, fairness and transparency apply to AI?
- ✓ How do we identify our purposes and lawful basis when using AI? And what should we consider when deciding lawful bases?
- ✓ How should we assess security and data minimisation in AI?
- ✓ How do individual rights apply to different stages of the AI lifecycle?

**Biometrics and Forensics Ethics Group Facial Recognition Working Group, January 2021**

https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing- note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology- accessible

The Biometrics and Forensics Ethics Group (BFEG) was commissioned to investigate the ethical issues raised by the collaborative use of live (real-time) biometric facial recognition technology (LFR) by public (police) and private organisations. Its briefing note provides a summary of the evidence gathered by the working group. It focuses on the use of LFR in a range of privately- owned spaces where people are gathered or are passing through (for example, shops and shopping centres) including those with clearly defined transit points where people are 'channeled' past the cameras (for example, within airports).

**Cardiff University - Evaluating the Use of Automated Facial Recognition Technology in Major Policing Operations – September 2018**

This report details findings from an evaluation of South Wales Police's deployment, conducted by Cardiff University, of Automated Facial Recognition between May 2017 and March 2018.

It reports that during the evaluation period, no overt racial discrimination effects were observed. However, this could potentially be an artefact of the demographic make-up of the Watchlists utilised.

http://afr.south-wales.police.uk/cms-assets/resources/uploads/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf

**Ada Lovelace Institute – Beyond face value: public attitudes to facial recognition technology, Sept 2019**

Published by the Ada Lovelace Institute, this survey shows that the British public are prepared to accept use of facial recognition technology in some instances, when there is a clear public benefit and where appropriate safeguards are put in place, but they also want the government to impose restrictions on its use.

Most people think facial recognition technologies should be permitted for use by police in criminal investigations (70%).

Ada Lovelace Institute- Ada's Citizens' Biometrics Council – Published in March 2021this paper reports on the debate on technologies that collect and process biometric data. The report makes 31 recommendations across a wide range of topics including: Independent oversight, legislation and regulation, data management, proportionality across different contexts, bias, discrimination and accuracy, consent and opt out and transparency

https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/

**Ada Lovelace Institute – The Citizens' Biometrics Council – March 2021**

Publication by Ada Lovelace institute this publication reports on the recommendations and findings of a public deliberation on biometrics technology, policy and governance.

The Citizens' Biometrics Council developed a set of recommendations to address the question: what is or isn't OK when it comes to the use of biometric technologies?

These recommendations cluster around three issues:
1. Developing more comprehensive legislation and regulation for biometric technologies.
2. Establishing an independent, authoritative body to provide robust oversight.
3. Ensuring minimum standards for the design and deployment of biometric technologies

https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf

**London Prepared – A city wide endeavour - Lord Toby Harris – March 2022**

An Independent Review of London's Preparedness to Respond to a Major Terrorist Incident.

In July 2021, the Mayor of London, Sadiq Khan, commissioned Lord Harris to undertake a new wide-ranging review of London's preparedness for a terrorist attack, against a backdrop of the changing nature of the threat of terrorism facing the capital. In the report Lord Harris has made 294 new recommendations that focus on several key areas including ensuring emergency services are properly funded and fully equipped, providing and refreshing specialist training for relevant teams to deal with specific types of attacks, and improving information sharing across those with a role to play in keeping London safe - many of these represent simple adjustments to existing processes. Specific inclusion of Live Facial Recognition Technology (referred to as AFR in the report) is highlighted in section 22.26 to 22.39 (inc). Lord Harris states "persuaded of the potential value of AFR in terms of preparedness for a terrorist attack – certainly its capacity to scan millions of images in real time means it has potential to augment human capabilities at significant pace and scale." And formally recommends "Any use of AFR by the MPS must be overseen by an Ethics Panel and there must be review mechanisms in place (R288) to ensure any implementation and operational issues are identified and reconciled as quickly as possible, with mitigations in place to manage the risk of unintended consequences"

**London Police Ethics Panel – Final Report on Live Facial Recognition – May 2019**

http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

Research was carried out on behalf of the London Policing Ethics Panel, the (London) Mayor's Office for Policing and Crime and the University College London Institute for Global City Policing by Opinion Research Services. This survey was not national but weighted to provide a representative sample of London's population. This survey found broad support for the use of LFR for policing purposes, with 57% of all those surveyed agreeing that it was acceptable for the MPS to use LFR. However, majorities of Asian (56%) and black (63%) people surveyed were opposed. Support is also lower amongst young people in London, with 55% of 16-24 and 52% of 25-39-year-olds opposed to the police use of LFR.

Views on using LFR to identify people wanted by the police vary considerably according to the seriousness of the crime. In the case of serious crimes, support varied between 83-81% depending on the nature of the threat; for minor crimes it falls to 55%, and below 50% for dealing with nuisance behaviour.

If it can be demonstrated from the trials there are clear and legitimate benefits to be gained from using LFR in defined circumstances, the Panel would favour proceeding by way of self-regulation and procedures that promote openness, transparency, and accountability.

The London Police Ethics Panel (LPEP), reviewed the way the Metropolitan Police were using facial recognition technology in 2025 since their initial report in 2019. Surveys indicate that many Londoners continue to support LFR when used for safety and crime prevention. The 2025 Public Attitude Survey found 85% of Londonders support police use of LFR, with the MPS making over 1400 arrests through its use of LFR. The Ethic Panels stance is best described as 'conditional acceptance requiring strong safeguards.'

policingethicspanel.london/uploads/4/4/0/7/44076193/london_policing_ethics_panel_-_live_facial_recognition_-_second_report.pdf

**South Wales Police Automated Facial Recognition website**

http://afr.south-wales.police.uk/

A public-facing website sharing information about facial recognition and South Wales Police's use of it. The site supplies information such as FAQ's, truths about the system, accuracy information and who they are seeking with this technology.

The website also lists future locations where the technology is due to be deployed. To aid transparency it also links to statistical pages where the public can examine the results of each Deployment.

**The Essex Report**

https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

This report covers a number of points including:

✓ The recent emergence of regional police-established independent ethics panels, normally staffed on a voluntary basis by independent experts, demonstrating the law enforcement community's desire to gain guidance and resolve these issues.
✓ Human rights law provides an organising framework for the design, development and deployment of advanced technologies such as LFR. As such, it can play a key role in ensuring that police forces can indeed 'strike the right balance' referred to in *S and Marper*.
✓ Police uses of surveillance measures typically satisfy the legitimate aim test on the basis of protecting the public from serious crime and upholding public order and arguments concerning the legitimate aim pursued by LFR.

**High Court of Justice – Bridges v Chief Constable of South Wales Police**

https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

The courts have recently considered the use of South Wales Police's (SWP) trials of Automated Facial Recognition technology in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)*. The court concluded that the police's common law powers to use facial recognition technology were 'amply sufficient'. The court further considered the Human Rights points and decided that whilst Article 8 was engaged, the use of facial recognition technology was necessary and proportionate in the circumstances. The court described it as 'misconceived' to limit the use of facial recognition technology to serious crimes and accepted the following use cases could justify the use of facial recognition technology in the right circumstances where necessity could be made out:

a) persons wanted on warrants;
b) individuals who are unlawfully at large (having escaped from lawful custody);
c) persons suspected of having committed crimes;
d) persons who may be in need of protection (e.g. missing persons);
e) individuals whose presence at a particular event causes particular concern;
f) persons simply of possible interest to SWP for intelligence purposes;
g) vulnerable persons.

Identifying a number of important safeguards to the use of LFR including with regards to the Public Sector Equality Duty, the court dismissed the challenge on all grounds and found the use of LFR in the case to be lawful. This judgement is now subject to an appeal which is not likely to be heard until late 2020. Refer to the MPS response to LPEP recommendations for further detail on the legal basis, necessity and proportionality.

**Court of Appeal – Bridges v Chief Constable of South Wales Police**

https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

The Court of Appeal recognised the legal framework for forces to use facial recognition but found the SWP left too much to officer discretion when considering who could be on a Watchlist and where SWP could deploy their AFR system. This means the deployments in question were not in accordance with the law for the purposes of Article 8. For SWP, this is can be remedied by providing sufficient detail in local force policy in a way that is clearly understandable and objective to answer (i) who can be on a Watchlist and (ii) where can LFR be deployed.

The Court found that SWP did not have a sufficient Data Protection Impact Assessment – the level of discretion given to officers meant that the use of AFR was not in accordance with the law. SWP also failed to consider the rights of those passing the LFR system (collateral intrusion). Consequently, the Data Protection Act 2018 was also breached.

The Court found that SWP did not pay due regard to the public sector equality duty. They had not updated their equality impact assessment form its initial issue and SWP had not taken measures to assure themselves as to whether their system had a gender or race bias in it prior to its use. Forces will need to reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm does not have an unacceptable bias.

**High Court – Thompson and Carlo v Commissioner of Police of the Metropolis**

The High Court considered whether the MPS policy governing the use of Live Facial Recognition (LFR) provided sufficient safeguards and limits on police discretion. Shaun Thompson and Silkie Carlo argued that the MPS retained too much discretion over where LFR could be deployed, why it could be deployed and who could be placed on a Watchlist, meaning its use was not sufficiently foreseeable or protected against arbitrary decision-making. The challenge was brought under Articles 8, 10 and 11 ECHR. Importantly, the claimants did not argue that police use of LFR was unlawful in principle.

The Court dismissed the challenge. It found that the MPS's revised September 2024 LFR policy provided a sufficiently clear legal framework and adequate safeguards to satisfy the requirement that interference with Convention rights is"in accordance with the law" / "prescribed by law." The Court emphasised that police discretion is not itself unlawful. The issue is whether that discretion is sufficiently structured and constrained to protect against arbitrary decision-making. It concluded that the MPS framework met that standard.

**FRA European union agency for fundamental rights – Facial recognition technology: Fundamental rights considerations in the context of law enforcement.**

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

This focus paper explores fundamental rights implications that should be taken into account when developing, deploying, using and regulating facial recognition technologies. It draws on recent analyses and data and evidence from interviews conducted with experts and representatives of national authorities who are testing facial recognition technologies.

✓ The paper forms part of FRA's larger research project on artificial intelligence, big data and fundamental rights. Of note from this paper. The high level of attention given to facial recognition technology in the recent past stems from strong accuracy gains achieved since 2014.

✓ At the same time, facial recognition technology can offer more timely protection – for example by helping to find missing children – and can help to detect fraud and identify theft.

✓ In relation to automated decision making and right to human review - Article 22 of the GDPR and Article 11 of the Law Enforcement Directive generally forbid automated decision making. Automated decision making is defined as a "decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

✓ In addition, as the child grows and time passes, the accuracy of a biometric match diminishes. The risk of a wrong match increases when facial images recorded at a young age are compared more than five years after they were collected. Present technologies for facial recognition guarantee a reliable match when the child was at least six years old when the biometric facial image was captured and the match happened within a time frame of five years. In general, research indicates that the accuracy of facial recognition technology is significantly lower for children younger than 13 years.

✓ Facial recognition technology algorithms never provide a definitive result. In the MPS, LFR is used to Alert officers of a possible match between a person passing the LFR system and a person on the Watchlist rather than definitively identifying those passing the LFR system. In the context of law enforcement, there is thus a certain margin of error leading to people being wrongly flagged. When deploying the technology, the risks of wrongly flagging people must be kept to a minimum. Everyone who is stopped as a result of the technology must be treated in a dignified manner.

✓ A fundamental rights impact assessment is an essential tool to ensure a fundamental rights compliant application of facial recognition technologies, whatever the context in which it is employed. Such an assessment needs to evaluate all affected rights, including those listed in this paper, in a comprehensive manner. To enable them to carry out such assessment, public authorities need to obtain all necessary information from the industry which is required

✓ to assess the technology's impact on fundamental rights. Trade secrets or confidentiality considerations should not hinder this effort.

**NIST Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories.

Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.

This is the third in a series of reports on ongoing face recognition vendor tests (FRVT) executed by NIST). In relation to these reports, the NIST Test report published in 2018[1] evaluated over 200 algorithms for their accuracy. Its findings state that:

*"NEC, which had produced broadly the most accurate algorithms in 2010, 2013, submitted algorithms that are substantially more accurate than their June 2018 versions and on many measures are now the most accurate"."*

In March 2017, NIST also published a Face In Video Evaluation (FIVE) report.[2] Unlike the other NIST Tests, the FIVE test involved the use of video footage as opposed to static images. This is of particular interest to the Met because this aligns more closely to the Met's use of facial recognition in a 'live' - video context. The NEC algorithm was found to be the most accurate across the different measures with a True Positive Identification rate of 82% at a corresponding False Positive Identification Rate of 0.4%.

In 2019, NIST published the first study to assess whether demographics such as gender or ethnicity cause FR Identification system accuracy to vary. 3 Tests were run on a 2.6 million image dataset where images were balanced with respect to representation of gender and ethnicity. The NIST results demonstrate that not all algorithms show uniform accuracy levels across the different demographics. However, NEC, the vendor used by the Met was found to perform well, with NIST saying that NEC had:

*"provided an algorithm for which the false positive differential was undetectable"* and the NEC-3 algorithm "*is on many measures, the most accurate [NIST] have evaluated*".

**Home Office Biometrics Strategy**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

The Home Office Biometrics Strategy sets out the overarching framework within which organisations in the Home Office sector will consider and make decisions on the use and development of biometric technology.

There are robust governance and oversight arrangements for well-established biometrics, and the Home Office is committed to developing this framework to ensure the effective governance of new biometric technologies.

✓ The use of biometric data is fundamental to the proper functioning of our immigration system, to law enforcement and to those responsible for preventing terrorism.

✓ As the technology develops this creates opportunities to not only improve safety and security, but to also deliver new and modern services.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf

[2] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

✓ Biometrics have long provided a critical role across the Home Office sector from traditional policing forensics,

immigration services to national security. The most commonly used forms of biometric are Deoxyribonucleic acid (DNA), fingerprints and face. In 2017, biometrics helped to facilitate the movement of over 46.2 million people through the ePassport Gates at our borders, supported 2.7 million visa applications and in 2016-17 helped to link over 32,000 known individuals to crimes including over 700 rapes.

✓ Biometrics – the recognition of people based on measurement and analysis of their biological characteristics or behavioural data – is increasingly prevalent in everyday life. It is used extensively by businesses to provide new and more efficient services, from unlocking mobile phones to secure banking.

✓ The face is the primary means used to identify people in many settings. Since the advent of photography, it has been extensively used by police officers and witnesses to identify suspects, or to verify people in immigration and nationality systems. Digital facial images are now used extensively when issuing documents that set out the holders' status, in the verification of identity and in the control of migration, often alongside fingerprints. The police capture facial images under powers set out in the Police and Criminal Evidence Act (PACE) 1984 and these are used in the investigation, detection and prevention of crime and terrorist activities as well as safeguarding.

**Home Office Biometrics Strategy**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_ Biometrics_Strategy_-_2018-06-28.pdf

The Home Office Biometrics Strategy sets out the overarching framework within which organisations in the Home Office sector will consider and make decisions on the use and development of biometric technology.

There are robust governance and oversight arrangements for well-established biometrics, and the Home Office is committed to developing this framework to ensure the effective governance of new biometric technologies.

✓ The use of biometric data is fundamental to the proper functioning of our immigration system, to law enforcement and to those responsible for preventing terrorism.

✓ As the technology develops this creates opportunities to not only improve safety and security, but to also deliver new and modern services.

✓ Biometrics have long provided a critical role across the Home Office sector from traditional policing forensics, immigration services to national security. The most commonly used forms of biometric are Deoxyribonucleic acid (DNA), fingerprints and face. In 2017, biometrics helped to facilitate the movement of over 46.2 million people through the ePassport Gates at our borders, supported 2.7 million visa applications and in 2016-17 helped to link over 32,000 known individuals to crimes including over 700 rapes.

✓ Biometrics – the recognition of people based on measurement and analysis of their biological characteristics or behavioural data – is increasingly prevalent in everyday life. It is used extensively by businesses to provide new and more efficient services, from unlocking mobile phones to secure banking.

✓ The face is the primary means used to identify people in many settings. Since the advent of photography, it has been extensively used by police officers and witnesses to identify suspects, or to verify people in immigration and nationality systems. Digital facial images are now used extensively when issuing documents that set out the holders' status, in the verification of identity and in the control of migration, often alongside fingerprints. The police capture facial images under powers set out in the Police and Criminal Evidence Act (PACE) 1984 and these are used in the investigation, detection and prevention of crime and terrorist activities as well as safeguarding.

**A New Met for London**

The MET Commissioner, Sir Mark Rowley is clear that the MPS's mission is to deliver More Trust, Less Crime, High Standards.

A comprehensive plan to build A New Met for London where communities know their local officers, help to shape their priorities and work with them to reduce crime and anti-social behaviour; and when victims call us for help, they're satisfied with our response. We'll build on the work we've done and keep serious violence low. We'll solve more rapes, domestic violence, child abuse and other cases of predatory offending, and we'll target the most dangerous offenders to take them off the streets before they can harm again. We'll reduce disproportionality when crime and our use of powers falls unevenly across London's communities.

https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/a-new-met-for-london/a-new-met- for-london.pdf

New Met for London Phase 2

In 2025 the Metropolitan Police Commissioner launched A New Met for London 2 as a continuation of NMfL. The MPS announced 1000 extra criminals were arrested every month with a a 16% reduction in neighbourhood crime in the first quarter of 2025/26. Twice as many crimes linked to VAWG were solved, along with 92% more shoplifting cases.

**Mayor of London – Building a Safer London - Police and Crime Plan 2022-25**

https://www.london.gov.uk/publications/building-safer-london

Mayor of London setting out his policing plan for London. This report raises the following priorities

The Mayor's vision is that London is a safe city for all. The Mayor wants London both to be a safer city and for Londoners to feel safer.

- ✓ Reducing and preventing violence
- ✓ Increasing trust and confidence
- ✓ Better supporting victims
- ✓ Protecting people from exploitation and harm

The Mayor's Police and Crime Plan 2025-2029 | London City Hall

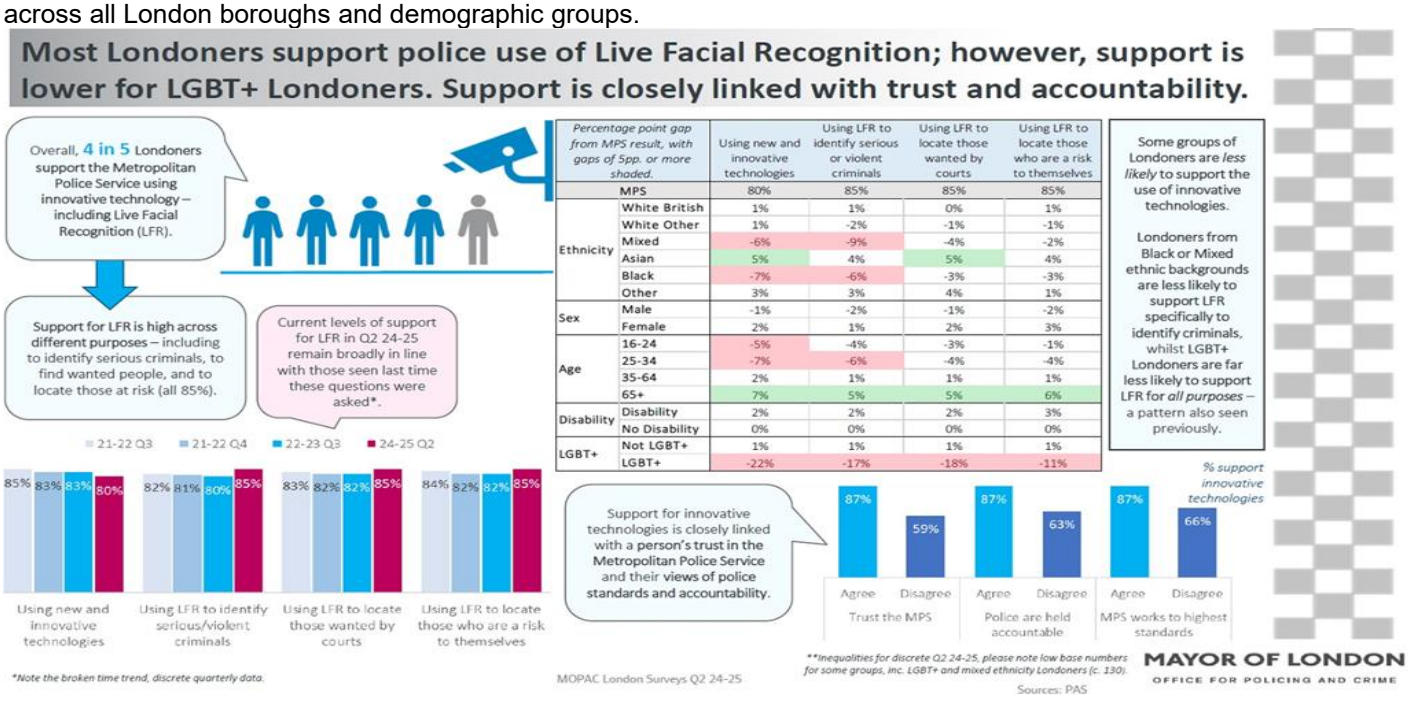
The Mayor of London set out his policing plan for London. This report raises the Mayor's agenda, to make London a safer city for all, by being tough on crime and tough ojn the complex causes of crime.

**The key aims of the Plan are:**

- **Reducing violence and criminal exploitation**
- **Building safer, more confident communities**
- **Supporting and overseeing reform of the MPS; and**
- **Improving the criminal justice system and supporting victims**

**MOPAC London Surveys Q2 24 25: MPS Use of innovative technology**

In addition to direct community engagement, the MPS also gathers formal feedback through commissioned surveys, such as the MOPAC Public Attitude Surveys (PAS). For example, results published in February 2025 showed that four in five Londoners support the use of innovative policing technologies, including LFR. Importantly, majority support was consistent across all London boroughs and demographic groups.



**MPS Data and Insight Hub**

Offender Management:

Identifies the number of outstanding suspects who are wanted by the MPS. The MPS has a statutory duty to prevent and detect crime. In order to fulfil that duty it is a priority for the MPS to detain and arrest those who are wanted as soon as possible. The number of wanted persons fluctuates on a daily basis and at any one time it is currently in the region of 15,000 persons who are being sought by the MPS.

Violent Crime:

- Since 1995 there have been 4,197 murders in London. In the *calendar year 2025 there were 93 Murders in London, and 81 recorded in 2026 (This figure is accurate as of 26 October 2026).*
- *In 2025 there were 1758 Gun Crime Offences in London.*
- *In 2025 there were 13812 recorded knife crimes.*
- *In the last 12 months there were 920,036 notifiable offences.*

**MPS Safeguarding Policy**

Policing vulnerable people demands close cooperation within the service and with key statutory partners in health and social care. London's partnership operating context is particularly complex, but the new MPS framework allows effective tiered engagement with police and partners at national, pan-London and local levels.

Working Together describes the categories of abuse as follows:

- ✓ Physical Abuse
- ✓ Emotional Abuse
- ✓ Sexual Abuse
- ✓ Neglect

Working together to safeguard children 2023: statutory guidance

**Biometrics commissioner interim report**

The report highlights ongoing challenges in oversight of biometric technologies, including facial recognition, during a period of organisational uncertainty and transition. It notes gaps in transparency and accountability, with the outgoing Commissioner stating that some information required for effective oversight has become "impossible to obtain," and emphasises that the governance framework for biometrics and surveillance cameras—facial recognition included—needs clearer guidance, stronger scrutiny, and investment, particularly around National Security Determinations (NSDs) and the broader regulation of surveillance tools. The report frames this moment as an opportunity to redesign how biometrics governance operates, ensuring more robust, well tested advice and safeguards around technologies such as facial recognition.

Biometrics and Surveillance Camera Commissioner's annual report 2023 to 2024 (accessible) - GOV.UK

**Surveillance Camera Commissioner "Facing the camera" document. November 2020**

The SCC is the independent regulator of the overt use and public operation of surveillance camera systems by the police in England and Wales. This includes systems incorporating LFR. The former SCC published a document outlining what is a good practice and guidance for the police use of overt surveillance camera systems incorporating facial recognition technology to locate persons on a Watchlist.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

**UK Commissioner defends face biometrics use by police as practical necessity**

Police have no choice but to use facial recognition, along with any other technologies that can help them fight crime, the UK's new Biometrics and Surveillance Camera Commissioner - Fraser Sampson

https://www.biometricupdate.com/202105/uk-commissioner-defends-face-biometrics-use-by-police-as-practical-necessity

**Biometrics & Surveillance Camera Commissioner Annual report – Jan 2021 – March 2022**

Biometrics & Surveillance Camera Commissioner Annual Report 2021-22 (publishing.service.gov.uk)

This 2021/2022 combined report is the first combined report that includes the respective responsibilities of both the Biometrics and Surveillance Camera Commissioners. . It covers issues relating to the PoFA regime in policing, the opportunities presented by new technological capabilities and their potential for improving police efficiency and effectiveness. It also highlights many of the risks and societal concerns that accompany those opportunities – particularly in the area of facial recognition technology and artificial intelligence. The report also recognises there remains a clear gap between how facial recognition technology is being used and how it is perceived as being used.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942155/Commissioner_for_the_retention_and_use_of_biometric_material_-_Interim_Report_December_2020___002_.pdf

**Minderoo Centre for Technology and Democracy – Oct 2022**

In this new report, researchers develop "minimum ethical and legal standards" for the governance of facial recognition technology and test them on three British police deployments. The audit extended to all types of facial recognition for identification, including live, retrospective, and mobile phone facial recognition. This audit was developed using a review of existing literature and feedback from academia, government, civil society, and police organisations on the ethics and legality of adopting facial recognition technology.

MCTD-FacialRecognition-Report-WEB-1.pdf

**HMICFRS - Getting the balance right? An inspection of how effectively the police deal with protests**

On 21 September 2020, the Home Secretary commissioned HMICFRS to conduct an inspection into how effectively the police manage respond to protests. This followed several protests, by groups including Extinction Rebellion, Black Lives Matter and many others. The Home Secretary required HMICFRS to assess the extent to which the police have been using their existing powers effectively, and what steps the Government could take to ensure that the police have the right powers to deal with protests.

In recent years, increasing amounts of police time and resources have been spent dealing with protests. In April and October 2019, Extinction Rebellion brought some of London's busiest areas to a standstill for several days. The policing operation for the two extended protests cost £37m, more than twice the annual budget of London's violent crime taskforce.

HMICFRS made a number of recommendations and areas for improvement and are designed to help the police get the balance right.

These included: Supporting forces to use live facial recognition technology in a way that improves police efficiency and effectiveness, while addressing public concerns about the use of such technology.

https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/getting-the-balance-right-an-inspection-of-how-effectively-the-police-deal-with-protests/

**If there is anything you are unsure of in this first section you can contact the Strategic Inclusion and Diversity Unit for further information and advice.**

## STEP 5. Full Impact Assessment Process

### STEP 5a. Consultation Log

GUIDANCE

Where are the consultation records stored? (e.g. General Registry, S-Drives etc)

S-Drive / One drive:

| Name of Business Group / Unit, Association, Stakeholder (External) | Why are you approaching / not approaching them? | Date and method of planned consultation | Outcome of consultation |
|---|---|---|---|
| **MPS Strategic Advisory Group** | To seek guidance and consult on the ethical views of the group for the proposed use of this technology. | 11th March 2021 | Positive outcome. Any concerns addressed during call. Some addition conversations offered if required. Agreed to return to the group in the future to update on the progress. |
| **MOPAC** | The MPS are accountable to MOPAC who provide London-wide policing priorities.<br><br>Early Engagement over the concept of implementation.<br><br>To seek views to support procedural best practice | 2016 - 2020 on going consultations.<br><br>2026 – Quarterly Cadence of MPS FRT Boards | MOPAC are represented at the MPS FRT Strategic Board.<br><br>Consultation has taken place with MOPAC regularly at the MPS FRT Strategic Board in specific relation to OIFR with this a standing agenda item |
| **National Institute of Standards and Technology** | To seek data on the existence of any bias regarding the accuracy of facial detection alert results across diverse facial variants.<br><br>To seek confirmation of the ability to effectively capture and monitor diversity data to determine the existence of future bias across facial detection accuracy. | Ongoing monitoring of relevant NIST output: 2016 – To date | Published comprehensive, independent, scientific literature which contains detailed reliable conclusions regarding demographic findings. |

| | | | |
|---|---|---|---|
| **Home Office Biometric Programme** | To seek views to support procedural best practice within the legal framework. | Ongoing consultations between 2016 to date. | Ongoing consultation |
| **National Police Chiefs Council** | Discussion and advice over the development of the project in its phases and the use of custody image. | Ongoing consultations between 2016 to date | Support and consistency at a national level. |
| **Civil Society Groups (Liberty, Privacy International, Big Brother Watch and Defend Digital Me)**<br><br>**Regulators (The Equality and Human Rights Commission, The ICO and The Biometrics and Surveillance Camera Commissioner)** | Engaged with to discuss the use of and the OIFR Policy Framework | June 2026 | A range of topics were discussed in relation to OIFR over the two engagement sessions. Points raised were focussed around, why deploy OIFR now. Making sure that the right safeguards were built into Policy framework. That the public were fully informed post use. The deletion of imagery taken and the use of image reference libraries. The impact and totality of other Facial Recognition tactics running concurrently. |
| **MPS Independent Advisory Groups (IAG) – Race IAG, LGBTQ+ IAG & Disability IAG.** | MPS IAG attendees consist of members of the public representing the protected characteristics of race, disability, sexual orientation and gender.<br><br>Consulted to attain public view points and assist with the identification of equality impact.<br><br>Central Race IAG | Ongoing consultation<br><br>21st August 2023 | Members were given an update on the MPS current position in respect to OIFR. Their views and feedback was sought in relation to the potential procurement and any views on the potential' custody use case'. Comments were supportive with a small number clarification points being raised about how, if any, data is retained and potentially used. IAG representative raised the following concerns:<br><br>▪ The retention of images/data<br>▪ The existence of ethnic bias<br>▪ Transparency<br>▪ Public Trust<br>▪ Necessity<br><br>The IAG representatives offered feedback on potential different community perspectives of OIFR and were pleased with the safeguards. Updates given to the group in relation to proposed use, functionality, policy and safeguarding.<br><br>Members were given a point of contact to liaise with should they have any further points to raise or if further clarification is needed. |

| | | | |
|---|---|---|---|
| | | 18th August 2026 | Presentation given on FR capabilities of MPS. Q & A session took place. Number of points were clarified for the group. Accuracy and bias of system discussed and recent NPL reporting highlighted.<br>Group broadly supportive of the technology.<br><br>Group to be given a demonstration in October 2023 at NSY of the technologies available.<br><br>October 2026<br><br>The Central Race IAG had a presentation delivered in October 2026, this specifically focussed on the Proof of Concept of OIFR. There were a number of questions in relation to the use, with some key areas around legal power and retention of imagery. |

| | | | |
|---|---|---|---|
| **Independent Advisory Groups and Safer Neighbourhood Boards – London Boroughs** | To seek views and show openness and transparency around FR technology | Ongoing across all 32 London Boroughs | Engagement sessions have taken place across all 32 London Boroughs, where IAG's, SNB's and elected members are engaged with.<br>These sessions take a cadence in line with the needs of the Borough and explain all uses of Facial Recognition technology, both of what is currently in use, but also highlighting the usage of OIFR across the MPS.<br><br>Support in the use of Facial Recognition technology varies from Borough to borough, but with general support in the MPS' use.<br><br>Areas of concerned that are often raised are in relation to<br><br>• Ethnic Bias and disproportionality in use<br>• Data retention<br>• Who is on the watchlist/image reference library<br>• How will the technology be used (use cases)<br><br>All engagements have enabled the MPS to inform the safeguards, mitigations and independent testing that has/is taking place, giving a a greater understanding of the MPS use of all FR technology. |

| | | | |
|---|---|---|---|
| **South Wales Police FRT Team** | SWP have implemented facial recognition technology trials (LFR and a fully operational OIFR system. MPS have conducted a bench marking exercise to discuss their governance and SOPs, to evaluate best operational practice. | Ongoing consultations between 2019-to date | Engagement continues with SWP at a both a national (NPCC) and force level to ensure best practice. |
| **Ada Lovelace Institute (ALI)** | The Ada Lovelace Institute is an independent research and deliberative body with a key mission to ensure data and AI work in the best interests of people and society.<br><br>Discussions to understand the main messages they report from their survey of public attitudes to the use of Facial Recognition in the UK. Their report was published in Sep 2019.<br><br>In March 2021 The institute published a further report via their Citizens Biometrics Council. This detailed the recommendations and findings of a public deliberation on biometrics technology, policy and governance.<br><br>That document includes references to FR technologies. | Ongoing consultations between 2019- to date | The MPS has actively engaged with ALI and considered their recommendations in line with their 3 key Aims.<br><br>The MPS SRO was and expert speaker, part of the oversight group and peer reviewed the March Citizen Biometrics Council document. |
| **Frontline Policing Headquarters** | Consult on the implementation of FR on their impacted business area. | Ongoing | Supported the concept of FR in meeting safeguarding policing priorities. |
| **Directorate of Legal Services** | To review the EIA and OIFR Proposal for legal compliance against the 'PSED' | Ongoing | Ongoing consultation |
| **London Policing Ethics Panel (LPEP)** | To attain LPEP's ethical framework considerations on LFR implementation. To seek views to support procedural best practice | Ongoing | Ongoing consultation and engagement |

| | | | |
|---|---|---|---|
| **Defence Science and Technology Laboratory** | Collaboration on working mechanics of testing and technological deployment.<br><br>Advice around academic documentation supporting the proof of concept of the product. Seek data on the existence of any bias regarding the accuracy of facial detection alert results across diverse facial variants.<br><br>To seek confirmation of the ability to effectively capture and monitor diversity data to determine the existence of future bias across facial detection accuracy | Ongoing | Ongoing consultation and engagement |
| **MPS Crime Prevention, Inclusion & Engagement Team (CPIE)** | Consult on the implementation of OIFR on their impacted business area | Ongoing | Ongoing consultation and engagement inc with a wider variety of CPIE stakeholders. |
| **Information Commissioner Office** | To seek guidance and consult on the ethical and legal practice of information management regarding this proposal an official regulatory body. To seek their views regarding the completion of the DPIA. To seek views to support procedural best practice within the legal framework. | Ongoing consultations between 2016-to date. | The use of OIFR involves the processing of personal data and therefore data protection law applies, whether it is for a trial or routine operational deployment. The ICO are consulted on outcome guidance and discussion to inform policy.<br><br>The processing of personal data by 'competent authorities' (s30 DPA 2018) for 'the law enforcement purposes' (s31 DPA 2018) is covered by Part 3 of the DPA 2018.<br><br>Specifically, the use of OIFR for the law enforcement purposes constitutes 'sensitive processing' (s35 (8)(b) DPA 2018) as it involves the processing of biometric data for the purpose of uniquely identifying an individual.<br><br>Such sensitive processing relates to all facial images captured and analysed by the software; and must pay particular attention to the requirements of s35, s42 and s64 DPA 2018. As such, a Data Protection Impact Assessment (DPIA) and an 'appropriate policy document' must be in place.<br><br>Sensitive processing occurs irrespective of |

| | | | |
|---|---|---|---|
| | | | whether that image yields a match to a person on a image reference library not. However, the biometric data of unmatched persons is deleted in line with MPS OIFR Policy.<br><br>Data protection law applies to the whole process of FR, from consideration about the necessity and proportionality for deployment, the compilation of image reference libraries and the processing of the biometric data through to the retention and deletion of that data. |
| **MPS Staff Support associations Association** | To gain insight on subject area based on consultants subject matter expertise to:<br><br>Assist with the identification of impact | 24/08/2020 – ongoing | Briefed on current position of FR use and all invited to launch of NPL Equitability Study. |

## STEP 5b. EIA Action Plan

**From your consultation activities and available information explain within the appropriate Action Plan Template the potential positive and / or negative impact of the proposal / policy, internally on members of your workforce and externally on your communities / service delivery:**

| | | | |
|---|---|---|---|
| **Age** | **GUIDANCE** | **Race** | **GUIDANCE** |
| **Deaf and disabled / Disability** | **GUIDANCE** | **Religion or Belief** | **GUIDANCE** |
| **Gender Reassignment** | **GUIDANCE** | **Sex** | **GUIDANCE** |
| **Marriage and Civil Partnership (employment only)** | **GUIDANCE** | **Sexual Orientation** | **GUIDANCE** |

| | | | |
|---|---|---|---|
| **Pregnancy and Maternity** | **GUIDANCE** | **Other Issues** | **GUIDANCE** |

## STEP 5c. Action Plan Template Workforce Impacts (Internal)

**GUIDANCE**

| Potential positive / negative issues / impacts | Activity | Role Holder | Action By Date | Progress/Timescale/ Monitoring |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **AGE: MPS STAFF**<br><br>No Impact | The age of employability is set by national police recruitment guidelines (18 or over)<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of age.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | N/A | N/A | N/A |
| **SEX: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of gender.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | N/A | N/A | N/A |
| **SEXUAL ORIENTATION: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal | N/A | N/A | N/A |

| | | | | |
|---|---|---|---|---|
| | provision to submit application forms for specified roles within the business area who use OIFR irrespective of sexual orientation<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | | | |
| **TRANSGENDER: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of a person's gender or how they identify.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | N/A | N/A | N/A |
| **RELIGION OR BELIEF: MPS STAFF**<br><br>No Impact on Recruitment | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of person's religion or belief.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | N/A | N/A | N/A |

| | | | | |
|---|---|---|---|---|
| Operational Impact upon Deployment | Practicing Islamic staff and officers are required to pray five times a day as part of religious practice. There is an obligatory requirement within Islam to attend Friday Prayers (preferably in a mosque as part of a congregation).<br><br>Although there is no legal obligation to facilitate religious prayer, the MPS prides itself on being an inclusive employer.<br><br>The MPS understand the importance of maintaining a diverse representation to reflect the community in which we serve.<br><br>Therefore, any staff or officer who will likely use OIFR and who requires flexibility for religious observance will be considered and reasonable adjustments made where possible dependant on operational necessity factors. | | | |
| **RACE: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of a person's race<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | N/A | N/A | N/A |
| **PREGNANCY / MATERNITY: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved | N/A | N/A | N/A |

| | | | | |
|---|---|---|---|---|
| | recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of a person's race<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework. | | | |
| **CIVIL PARTNERSHIP: MPS STAFF**<br><br>No Impact | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be an equal provision to submit application forms for specified roles within the business area who use OIFR irrespective of a person's civil partnership status.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework.<br>specific performance framework | N/A | N/A | N/A |
| **DISABILITY: MPS STAFF**<br><br>Impacted<br><br>Training Provision for Diverse Learning Styles | The MPS is an equal opportunities employer.<br><br>The process of becoming an Authorised OIFR User will be role specific to each business area granted permission to use the technology. These business areas have their own approved recruitment policy. There will be equal provisions to submit application forms for specified roles within the business area who use OIFR irrespective if a person has a disability.<br><br>MPS recruitment processes are auditable, transparent and set to a rank specific performance framework.<br><br><u>Operational Requirements:</u> | N/A | N/A | N/A |

| | | | | |
|---|---|---|---|---|
| | Role requirements have been set in accordance with MPS Health & Safety Policy, HR Recruitment Policy and MPS Performance Framework.<br>https://www.met.police.uk/SysSiteAssets/foi-media/metropolitan-police/policies/strategy--governance---mps-health-and-safety-policy<br><br>https://portal.psop.policesharedservices.co.uk/km/recruitment-options-procedure/recruitment-options-procedures-managers-guide-police-officer-police<br><br>https://portal.psop.policesharedservices.co.uk/km/subject/36<br><br>Personnel who have a disability where their physical and/or mental impairment has a substantial and long-term adverse effect on their ability to carry out normal day-to-day activities will be supported via an Occupational Health Referral where reasonable adjustments will be recommended and the appropriate risk assessments completed.<br><br><u>Training Provision:</u><br><br>A Training course will be delivered by the chosen vendor covering the operational use of OIFR.<br>This could include a knowledge check test, and a handout for supplementary learning. This covers the four identified learning styles.<br><br>▪ Visual Learners<br>▪ Auditory Learners<br>▪ Read/Write<br>▪ Kinaesthetic<br><br>For personnel with a visual impairment, adaptations assistive technology follows MPS DDaT SOP's. | | | |

| | | | | |
|---|---|---|---|---|
| | For personnel with dyslexia appropriate assistive technology follows MPS DDat SOP's. | | | |

| STEP 5d. EIA Action Plan Template Service Delivery Impacts (External) | | | | GUIDANCE |
|---|---|---|---|---|
| Potential positive / negative issues / impacts | Activity | Role Holder | Action By Date | Progress/Timescale/ Monitoring |
| **AGE:**<br><br>Impacted<br><br>OIFR searches are based on the mapping of key facial indicators when comparing a Probe Image to an image from an authorised Image Reference Library.<br><br>Therefore, the functionality, accuracy and performance of OIFR may be less effective if changes to facial appearance have occurred between the time a Probe Image was taken, and the time that it is searched against an authorised Image Reference Library.<br><br>In addition, the European Union's Agency for Fundamental Rights 'Facial Recognition Technology Fundamental Rights Considerations in the Context of Law Enforcement Report 2019' highlights that as a child grows and time passes, the accuracy of a biometric match can diminish. The risk of failure to match increases when facial images recorded at a young age are compared more than five years after they were collected. The report further indicates that the accuracy of facial recognition technology *is in general* significantly lower for children younger than 13 years old. They associate this to "rapid growth and change in facial appearance".<br><br>OIFR images will be taken via a mobile application on a Met Police issued mobile phone. The operator will make use of a mobile application to take an image of the subject, the quality of this image taken will be assessed by the system and where the image falls below the system accepted | • **Performance**: The MPS uses an NEC-supplied facial recognition algorithm for OIFR. The algorithm has been independently tested by the National Institute of Standards and Technology (NIST), and the MPS has considered the results of that testing when assessing system performance. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance. The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability Study by the National Physical Laboratory included tested data from a wide of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| threshold, the image will not be processed and the operator will have the opportunity to retake the image of the subject..<br><br>There is a positive impact towards the early resolution of investigations relating to vulnerable children. OIFR has the capability to support safeguarding measures to reduce a child's exposure to CSE, abuse and/or neglect. | identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in day-to-day use of OIFR.<br><br>• **Policy Framework and Legal Safeguards**: The use of OIFR is governed by a comprehensive legal, policy and governance framework which establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br><br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the MPS OIFR Policy, Legal Mandate and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely on automated processing.<br><br>• **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy and governance requirements have been satisfied.<br><br>• Additional safeguards apply in relation to the use of Probe Images, including | | | |

| | | | | |
|---|---|---|---|---|
| | requirements relating to image quality, proportionality, necessity, protected characteristics and the use of images depicting young persons. These safeguards are set out within the MPS OIFR Policy and supporting operational procedures. OIFR Users must not undertake a search unless they are satisfied that all applicable safeguards have been met and where required (subject perceived age 13-17) the authority of a minimum rank of Inspector (or Police Staff equivalent) to authorise the use of OIFR.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches returned by the system are presented to a trained OIFR User for review. The OIFR User is responsible for independently assessing the results and determining whether any Potential Match may constitute a Viable Match.<br><br>• In undertaking this assessment, the OIFR User must consider all relevant subject, system and environmental factors that could affect the reliability of the result, including image quality, lighting conditions, time elapsed between images and age-related changes in appearance. OIFR Users must not assume that a highly ranked or visually similar result is a Viable Match.<br><br>• Where a Viable Match is identified, any subsequent policing decision must be based upon the totality of available information and intelligence and not | | | |

| | | | | |
|---|---|---|---|---|
| | solely upon the OIFR result. The level of documentation required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br><br>• A Viable Match constitutes an intelligence lead only and does not, in itself, amount to formal identification or evidential proof of identity.<br><br>• For example, the system may present subjects who appear noticeably older or younger than the person depicted in the Probe Image. Such differences do not automatically render a match non-viable, but the OIFR User must assess whether the apparent age variation can be explained by natural ageing, the time lapse between images, or other relevant factors.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold:** The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br><br>• The OIFR system incorporates a similarity score threshold designed to reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation of the OIFR System. By filtering lower-confidence results, the threshold helps reduce the risk of individuals being | | | |

| | | | | |
|---|---|---|---|---|
| | incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals.<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br>• Training includes the legal and ethical framework governing OIFR, operational procedures, system limitations, human review and adjudication requirements, equality considerations and diversity awareness. OIFR Users must maintain their competence in accordance with MPS training requirements.<br><br>• **Monitoring OIFR Viable Matches**: The MPS maintains records relating to OIFR Searches and outcomes to support governance, oversight, audit and compliance monitoring.<br>• Relevant information relating to searches, outcomes and demographic characteristics will be analysed to support ongoing assessment of operator performance, system performance, equality impacts and compliance with the Public Sector Equality Duty. | | | |

| | | | | |
|---|---|---|---|---|
| | • **Post OIFR Search Monitoring**: OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board..<br><br>Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. Findings may inform changes to policy, operating procedures, training, governance arrangements or system configuration where appropriate.<br><br>• **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br><br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting mechanisms. The MPS will maintain a record of composition of (i) sex (ii) race by IC Code and (iii) age range of OIFR searches. This may also include aggregated information relating to system use, outcomes and equality monitoring activities. | | | |

| | | | | |
|---|---|---|---|---|
| **SEX:**<br><br>**Impacted**<br><br>National Institute of Standards & Technology independent testing that have been undertaken on facial recognition algorithms with respect to demographic differentials (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, December 2019). NIST tests show a wide range in accuracy across different algorithms (including in relation to gender) and universal statements about 'bias' are not supported by testing.<br><br>From its own system data and the demographic analysis published on GOV.UK, the MPS is mindful of the profile of images contained within its Substantive Image Reference Libraries**,** which reflect the composition of those arrested (where there is a significant skew towards males) rather than the general population. As OIFR Searching draws from these Substantive Image Reference Libraries, the demographic distribution of returned Potential Matches may mirror the characteristics of the individuals lawfully captured and held within those libraries, rather than wider London demographics. | • **Performance**: The MPS uses an NEC-supplied facial recognition algorithm for OIFR. NEC's algorithms have been independently tested by the National Institute of Standards and Technology (NIST), and the MPS takes account of those results. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance.<br>• The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability Study by the National Physical Laboratory included tested data from a wide range of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in day-to-day use of OIFR.<br><br>• **Policy Framework and Legal Safeguards**: The use of OIFR is | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| | governed by a comprehensive legal, policy and governance framework that establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br><br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the OIFR Legal Mandate, OIFR Policy and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely upon automated processing.<br><br>• **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy and governance requirements have been satisfied.<br><br>• Additional safeguards apply in relation to the use of Probe Images and are set out within the MPS OIFR Policy and supporting operational procedures. These include safeguards relating to image quality, necessity, proportionality and the appropriate use of imagery. OIFR Users must not undertake an OIFR Search unless they are satisfied that all applicable safeguards have been met.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches are returned to the OIFR User for review. | | | |

| | | | | |
|---|---|---|---|---|
| | It is for the OIFR User to independently assess the results and determine whether any Potential Match may constitute a Viable Match.<br>• OIFR Users must not assume that a highly ranked or visually similar Potential Match is viable. In undertaking their assessment, they must consider all relevant subject, system and environmental factors that may affect the reliability of the result, including image quality, image age, lighting conditions and any other factors that may influence system performance.<br>• Where an OIFR User determines that a Potential Match constitutes a Viable Match, any subsequent policing decision must be based upon the totality of available information and intelligence and not solely upon the OIFR result. The level of documentation and audit recording required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br>• A Viable Match provides an intelligence lead only, requiring further investigative assessment that may ultimately support or undermine the initial assessment. A Viable Match does not constitute formal identification and cannot, by itself, be relied upon as evidence.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold:** The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br>• The OIFR system incorporates a similarity score threshold designed to reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is | | | |

| | | | | |
|---|---|---|---|---|
| | currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation of the OIFR System. By filtering lower-confidence results, the threshold helps reduce the risk of individuals being incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals.<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br>• Training includes the legal and ethical framework governing OIFR, operational procedures, system limitations, human adjudication requirements, equality considerations and diversity awareness. OIFR Users must maintain their competence in accordance with MPS requirements.<br><br>• **Post OIFR Search Monitoring**: OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board..<br><br>• Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. Findings may inform changes to policy, operating procedures, training, governance arrangements or system configuration where appropriate. | | | |

| | | | | |
|---|---|---|---|---|
| | • The MPS recognises that some Image Reference Libraries may contain a higher proportion of males than females. This is not a consequence of OIFR itself, but reflects the composition of images lawfully held by the MPS for policing purposes and the populations from which those images are derived. The MPS does not consider the composition of an Image Reference Library, in itself, to constitute unlawful discrimination. However, the MPS recognises that any disproportionate representation of individuals by sex may give rise to concerns regarding fairness, equality impacts and public confidence. The use of OIFR is therefore restricted to approved policing purposes and subject to legal, policy and governance controls designed to ensure that searches are undertaken only where lawful, necessary and proportionate.<br>• The MPS MO3 FR Team will monitor OIFR use and outcomes through its, including analysis of available demographic information relating to searches and outcomes. This monitoring will assist the MPS in identifying any emerging disproportionate impacts on individuals who share the protected characteristic of sex and, where appropriate, inform changes to policy, operational practice, training, governance arrangements or system configuration. | | | |

| | | | | |
|---|---|---|---|---|
| | • **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting mechanisms. The MPS will maintain a record of composition of (i) sex (ii) race by IC Code and (iii) age range of OIFR searches. This may also include aggregated information relating to system use, outcomes and equality monitoring activities. | | | |

| | | | | |
|---|---|---|---|---|
| **SEXUAL ORIENTATION:**<br><br>No impact – this assessment remains subject to specific equality impact considerations.<br><br>OIFR compares Probe Images to Image Reference Libraries using objective facial measurements. The system does not detect, infer or rely on any information relating to sexual orientation, and this protected characteristic has no effect on the facial indicators used for matching.<br><br>Sexual orientation does not alter facial structures in a way that affects image comparison; therefore, it has no bearing on OIFR functionality, accuracy, or performance. | | FR Team | Ongoing | |
| • **GENDER REASSIGNMENT:**<br><br>• Impacted<br><br>• OIFR searches are based on the mapping of key facial indicators when comparing a Probe Image to an image from an authorised Image Reference Library.<br><br>• Therefore, the functionality, accuracy and performance of OIFR may be less effective if changes to facial appearance have occurred between the time a Probe Image was taken, and the time that it is searched against an authorised Image Reference Library.<br><br>• This may impact persons who are transitioning from one legal gender to another if gender presentation differs from the time the comparator image was | • **Performance**: The MPS uses an NEC-supplied facial recognition algorithm for OIFR. The algorithm has been independently tested by the National Institute of Standards and Technology (NIST), and the MPS has considered the results of that testing when assessing system performance. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance. The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| taken.<br><br>• It may also affect trans, non-binary and gender- fluid people who adopt to flex between gender presentations.<br><br>• Reports suggest that facial contouring through the use of cosmetic make-up application or undertaking facial surgery may impact on the OIFR system's performance too. | testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability Study by the National Physical Laboratory included tested data from a wide of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in day-to-day use of OIFR.<br><br>• **Policy Framework and Legal Safeguards**: The use of OIFR is governed by a comprehensive legal, policy and governance framework which establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br><br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the MPS OIFR Policy, Legal Mandate and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely on automated processing. | | | |

| | | | | |
|---|---|---|---|---|
| | • **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy and governance requirements have been satisfied.<br><br>• Additional safeguards apply in relation to the use of Probe Images, including requirements relating to image quality, proportionality, necessity, protected characteristics and the use of images depicting young persons. These safeguards are set out within the MPS OIFR Policy and supporting operational procedures. OIFR Users must not undertake a search unless they are satisfied that all applicable safeguards have been met and where required (subject has undertaken gender reassignment) the authority of a minimum rank of Inspector (or Police Staff equivalent) to authorise the use of OIFR.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches returned by the system are presented to a trained OIFR User for review. The OIFR User is responsible for independently assessing the results and determining whether any Potential Match may constitute a Viable Match.<br><br>• In undertaking this assessment, the OIFR User must consider all relevant subject, system and environmental factors that | | | |

| | | | | |
|---|---|---|---|---|
| | could affect the reliability of the result, including image quality, lighting conditions, time elapsed between images and age-related changes in appearance. OIFR Users must not assume that a highly ranked or visually similar result is a Viable Match.<br><br>• Where a Viable Match is identified, any subsequent policing decision must be based upon the totality of available information and intelligence and not solely upon the OIFR result. The level of documentation required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br><br>• A Viable Match constitutes an intelligence lead only and does not, in itself, amount to formal identification or evidential proof of identity.<br><br>• For example, the system may present subjects who appear noticeably older or younger than the person depicted in the Probe Image. Such differences do not automatically render a match non-viable, but the OIFR User must assess whether the apparent age variation can be explained by natural ageing, the time lapse between images, or other relevant factors.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold:** The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br><br>• The OIFR system incorporates a similarity score threshold designed to | | | |

| | | | | |
|---|---|---|---|---|
| | reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation of the OIFR System. By filtering lower-confidence results, the threshold helps reduce the risk of individuals being incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals.<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br>• Training includes the legal and ethical framework governing OIFR, operational procedures, system limitations, human review and adjudication requirements, equality considerations and diversity awareness. OIFR Users must maintain their competence in accordance with MPS training requirements.<br>• **Monitoring OIFR Viable Matches**: The MPS maintains records relating to OIFR | | | |

| | | | | |
|---|---|---|---|---|
| | Searches and outcomes to support governance, oversight, audit and compliance monitoring.<br><br>• Relevant information relating to searches, outcomes and demographic characteristics will be analysed to support ongoing assessment of operator performance, system performance, equality impacts and compliance with the Public Sector Equality Duty.<br><br>• **Post OIFR Search Monitoring**: OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board..<br><br>• Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. Findings may inform changes to policy, operating procedures, training, governance arrangements or system configuration where appropriate.<br><br>• **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br><br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting | | | |

| | | | | |
|---|---|---|---|---|
| | mechanisms. The MPS will maintain a record of composition of (i) sex (ii) race by IC Code and (iii) age range of OIFR searches. This may also include aggregated information relating to system use, outcomes and equality monitoring activities. | | | |

| | | | | |
|---|---|---|---|---|
| • **RELIGION OR BELIEF:**<br><br>• Impacted<br><br>• National Institute of Standards & Technology independent testing that have been undertaken on facial recognition algorithms with respect to demographic differentials (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, December 2019). NIST tests show a wide range in accuracy across different algorithms and universal statements about 'bias' are not supported by testing.<br><br>• However, the functionality, accuracy and performance of OIFR may be less effective if the face is obstructed. Therefore, the wearing of religious headwear/ coverings and/or facial hair may have a bearing on OIFR and the operational decision to use this capability or not<br><br>• Risk of community tension. In addition, via consultation with the MPS Staff Associations have revealed that some religions have strict guidelines pertaining to photography. A lack of awareness around OIFR Probe Image use under these circumstances is likely to lead to discontent and/or community tension. | • **Performance**: The MPS uses an NEC-supplied facial recognition algorithm for OIFR. The algorithm has been independently tested by the National Institute of Standards and Technology (NIST), and the MPS has considered the results of that testing when assessing system performance. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance. The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability Study by the National Physical Laboratory included tested data from a wide of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in day-to-day use of OIFR.<br><br>• **Policy Framework and Legal** | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| | **Safeguards**: The use of OIFR is governed by a comprehensive legal, policy and governance framework which establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the MPS OIFR Policy, Legal Mandate and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely on automated processing.<br>• **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy and governance requirements have been satisfied.<br>• Additional safeguards apply in relation to the use of Probe Images, including requirements relating to image quality, proportionality, necessity, protected characteristics and the use of images depicting young persons. These safeguards are set out within the MPS OIFR Policy and supporting operational procedures. OIFR Users must not undertake a search unless they are satisfied that all applicable safeguards have been met and where required the authority of a minimum rank of Inspector | | | |

| | | | | |
|---|---|---|---|---|
| | (or Police Staff equivalent) to authorise the use of OIFR.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches returned by the system are presented to a trained OIFR User for review. The OIFR User is responsible for independently assessing the results and determining whether any Potential Match may constitute a Viable Match.<br><br>• In undertaking this assessment, the OIFR User must consider all relevant subject, system and environmental factors that could affect the reliability of the result, including image quality, lighting conditions, time elapsed between images and age-related changes in appearance. OIFR Users must not assume that a highly ranked or visually similar result is a Viable Match.<br><br>• Where a Viable Match is identified, any subsequent policing decision must be based upon the totality of available information and intelligence and not solely upon the OIFR result. The level of documentation required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br><br>• A Viable Match constitutes an intelligence lead only and does not, in itself, amount to formal identification or evidential proof of identity.<br><br>• For example, the system may present subjects who appear noticeably older or younger than the person depicted in the Probe Image. Such differences do not | | | |

| | | | | |
|---|---|---|---|---|
| | automatically render a match non-viable, but the OIFR User must assess whether the apparent age variation can be explained by natural ageing, the time lapse between images, or other relevant factors.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold**The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br><br>The OIFR system incorporates a similarity score threshold designed to reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation of the OIFR System. By filtering lower-confidence results, the threshold helps reduce the risk of individuals being incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br><br>• Training includes the legal and ethical | | | |

| | | | | |
|---|---|---|---|---|
| | framework governing OIFR, operational procedures, system limitations, human review and adjudication requirements, equality considerations and diversity awareness. OIFR Users must maintain their competence in accordance with MPS training requirements.<br><br>• **Monitoring OIFR Viable Matches**: The MPS maintains records relating to OIFR Searches and outcomes to support governance, oversight, audit and compliance monitoring.<br><br>• Relevant information relating to searches, outcomes and demographic characteristics will be analysed to support ongoing assessment of operator performance, system performance, equality impacts and compliance with the Public Sector Equality Duty.<br><br>• **Post OIFR Search Monitoring**: OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board..<br><br>• Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. Findings may inform changes to policy, operating procedures, training, governance arrangements or system configuration where appropriate.<br><br>• **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact | | | |

| | | | | |
|---|---|---|---|---|
| | assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br><br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting mechanisms. The MPS will maintain a record of composition of (i) sex (ii) race by IC Code and (iii) age range of OIFR searches. This may also include aggregated information relating to system use, outcomes and equality monitoring activities. | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| • **RACE:**<br><br>• Impacted<br><br>• National Institute of Standards & Technology independent testing that have been undertaken on facial recognition algorithms with respect to demographic differentials (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, December 2019). NIST tests show a wide range in accuracy across different algorithms and universal statements about 'bias' is not supported by testing. The MPS therefore needs to be alive to the risk that a facial recognition algorithm could perform differently across different racial groups and consideration as to whether to use this operational capability or not. | • **Performance** The MPS uses an NEC-supplied facial recognition algorithm for OIFR. The algorithm has been independently tested by the National Institute of Standards and Technology (NIST), and the MPS has considered the results of that testing when assessing system performance. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance. The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| | Study by the National Physical Laboratory included tested data from a wide of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in day-to-day use of OIFR.<br><br>• **Policy Framework and Legal Safeguards**: The use of OIFR is governed by a comprehensive legal, policy and governance framework which establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br><br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the MPS OIFR Policy, Legal Mandate and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely on automated processing.<br><br>• **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy | | | |

| | | | | |
|---|---|---|---|---|
| | and governance requirements have been satisfied.<br><br>• Additional safeguards apply in relation to the use of Probe Images, including requirements relating to image quality, proportionality, necessity, protected characteristics and the use of images depicting young persons. These safeguards are set out within the MPS OIFR Policy and supporting operational procedures. OIFR Users must not undertake a search unless they are satisfied that all applicable safeguards have been met and where required the authority of a minimum rank of Inspector (or Police Staff equivalent) to authorise the use of OIFR.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches returned by the system are presented to a trained OIFR User for review. The OIFR User is responsible for independently assessing the results and determining whether any Potential Match may constitute a Viable Match.<br><br>• In undertaking this assessment, the OIFR User must consider all relevant subject, system and environmental factors that could affect the reliability of the result, including image quality, lighting conditions, time elapsed between images and age-related changes in appearance. OIFR Users must not assume that a highly ranked or visually similar result is a Viable Match.<br><br>• Where a Viable Match is identified, any | | | |

| | | | | |
|---|---|---|---|---|
| | subsequent policing decision must be based upon the totality of available information and intelligence and not solely upon the OIFR result. The level of documentation required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br><br>• A Viable Match constitutes an intelligence lead only and does not, in itself, amount to formal identification or evidential proof of identity.<br><br>• For example, the system may present subjects who appear noticeably older or younger than the person depicted in the Probe Image. Such differences do not automatically render a match non-viable, but the OIFR User must assess whether the apparent age variation can be explained by natural ageing, the time lapse between images, or other relevant factors.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold:** The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br><br>• The OIFR system incorporates a similarity score threshold designed to reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation | | | |

| | | | | |
|---|---|---|---|---|
| | of the OIFR System. By filtering lower-confidence results, the threshold helps reduce the risk of individuals being incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals.<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br><br>• Training includes the legal and ethical framework governing OIFR, operational procedures, system limitations, human review and adjudication requirements, equality considerations and diversity awareness. OIFR Users must maintain their competence in accordance with MPS training requirements.<br><br>• **Monitoring OIFR Viable Matches**: The MPS maintains records relating to OIFR Searches and outcomes to support governance, oversight, audit and compliance monitoring.<br><br>• Relevant information relating to searches, outcomes and demographic characteristics will be analysed to support ongoing assessment of operator performance, system performance, equality impacts and compliance with the | | | |

| | | | | |
|---|---|---|---|---|
| | Public Sector Equality Duty. This monitoring will include consideration of whether particular racial groups are disproportionately represented in OIFR Searches, Viable Matches or subsequent policing outcomes, and whether any emerging disproportionality can be explained by legitimate operational factors, including the composition of approved Image Reference Libraries and the policing purpose for which OIFR is being used.<br><br>• **Post OIFR Search Monitoring**: : OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board..<br><br>• Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. This will include consideration of whether OIFR deployments, searches, viable matches or subsequent interventions have a disproportionate impact on individuals from particular racial groups. The MPS will seek to understand the causes of any identified disproportionality, including whether it is attributable to operational deployment decisions, the composition of approved Image Reference Libraries, policing demand, or system performance. Findings may inform changes to policy, operating procedures, training, | | | |

| | | | | |
|---|---|---|---|---|
| | governance arrangements or system configuration where appropriate.<br><br>• **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br><br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting mechanisms. The MPS will maintain a record of composition of (i) sex (ii) race by IC Code and (iii) age range of OIFR searches. This may also include aggregated information relating to system use, outcomes and equality monitoring activities. | | | |

| | | | | |
|---|---|---|---|---|
| **PREGNANCY / MATERNITY:**<br><br>No impact – this assessment remains subject to specific equality impact considerations.<br><br>OIFR searches are based on the mapping of key facial indicators when comparing a Probe Image to an image from an authorised Image Reference Library.<br><br>The functionality, accuracy and performance of OIFR have no bearing on an individual who are pregnant. | | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| The protected characteristic of Pregnancy and Maternity does not impede on changes and/or adaptations to a subject's face. | | | | |
| **MARRIAGE AND CIVIL PARTNERSHIP:**<br><br>No impact – this assessment remains subject to specific equality impact considerations.<br><br>OIFR searches are based on the mapping of key facial indicators when comparing a Probe Image to an image from an authorised Image Reference Library.<br><br>The functionality, accuracy and performance of OIFR have no bearing on an individual who are married or have entered a civil partnership.<br><br>The protected characteristic does not impede on changes and/or adaptations to a subject's face. | | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| **DISABILITY:**<br><br>Impacted<br><br>OIFR searches are based on the mapping of key facial indicators when comparing a Probe Image to an image from an authorised Image Reference Library.<br><br>Therefore, the functionality, accuracy and performance of OIFR may be less effective if changes to facial appearance have occurred between the time a Probe Image was taken, and the time that it is searched against an authorised Image Reference Library.<br><br>This may impact persons with facial disfigurement and/or facial structural changed through trauma, medical condition and/or intervention, or required to wear medical eyewear etc. However, defining structural facial features including the presence of marks and/or scars may also aid the accuracy of OIFR performance.<br><br>Consideration has also been given to the following identified impact:<br><br>• The camera angle for which the Probe Image was taken and the OIFR system's capability to Template persons with genetic and/ or medical conditions that impact on a person's height and/or wheelchair / mobility scooter users where this may impact on the Probe Image (e.g. from fixed CCTV).<br><br>• The accuracy of OIFR system in relation to facial disfigurement as a result of injury/trauma and/or disability. | • **Performance**: The MPS uses an NEC-supplied facial recognition algorithm for OIFR. The algorithm has been independently tested by the National Institute of Standards and Technology (NIST), and the MPS has considered the results of that testing when assessing system performance. The MPS has also undertaken its own testing and evaluation to understand the impact of subject, system and environmental factors on operational performance. The MPS publishes Understanding Accuracy and Demographic Differences, which provides a public explanation of the steps taken to assess statistical accuracy and demographic performance and to meet the Public Sector Equality Duty (PSED). The MPS keeps relevant research, testing and operational performance under review which will ensure OIFR continues to operate fairly, effectively and proportionately.<br><br>• The Facial Recognition Equitability Study by the National Physical Laboratory included tested data from a wide range of demographics and noted no statistically significant variance in performance across demographics. Additionally, the True Positive Identification Rate (TPIR) is identical for all demographic subgroups and, with no demographic performance variation in TPIR, performance is considered equitable. The MPS uses findings from independent studies to inform its assessment of fairness, equality impact and proportionality in the day-to-day use of OIFR.<br><br>• In relation to disability, the principal equality risks are not considered to arise primarily from algorithmic performance differences. Instead, potential impacts may arise where disability, injury, medical treatment or surgical intervention affects facial appearance, where it is more difficult to obtain suitable facial imagery, where disability-related factors affect image capture or image interpretation, or | FR Team | Ongoing | |

| | | | | |
|---|---|---|---|---|
| | where accessibility and engagement needs are not adequately considered. The MPS considers these factors when assessing the overall fairness, proportionality and equality impact of OIFR and implements additional safeguards to mitigate any potential adverse impacts.<br><br>• **Policy Framework and Legal Safeguards**: The use of OIFR is governed by a comprehensive legal, policy and governance framework which establishes requirements relating to legality, necessity, proportionality, accountability and human oversight.<br>• OIFR may only be used for approved use cases and against approved Image Reference Libraries. All OIFR searches must satisfy the requirements set out within the MPS OIFR Policy, Legal Mandate and associated governance documentation. These safeguards are designed to ensure that OIFR is used only in pursuit of a legitimate policing aim and that decisions are not based solely on automated processing.<br><br>• **Probe Image safeguards**: Every OIFR Search must be supported by an authorised OIFR submission process. This process requires confirmation that the proposed use falls within a permitted use case and that relevant legal, policy and governance requirements have been satisfied.<br>• Additional safeguards apply in relation to the use of Probe Images, including requirements relating to image quality, proportionality, necessity, protected characteristics and the use of images depicting young persons. These safeguards are set out within the MPS OIFR Policy and supporting operational procedures. OIFR Users must not undertake a search unless they are satisfied that all applicable safeguards have been met and, where required (a person with a relevant disability), the | | | |

| | | | | |
|---|---|---|---|---|
| | authority of a minimum rank of Inspector (or Police Staff equivalent) has been obtained to authorise the use of OIFR.<br><br>• **Officer engagement**: When an OIFR Search is undertaken, Potential Matches returned by the system are presented to a trained OIFR User for review. The OIFR User is responsible for independently assessing the results and determining whether any Potential Match may constitute a Viable Match.<br>• In undertaking this assessment, the OIFR User must consider all relevant subject, system and environmental factors that could affect the reliability of the result, including image quality, lighting conditions, time elapsed between images and age-related changes in appearance. OIFR Users must also consider whether disability, injury, medical treatment or surgical intervention may have affected an individual's facial appearance. Examples may include facial disfigurement, burns, reconstructive surgery or certain medical conditions which may alter or affect facial features over time.<br>• OIFR Users must additionally consider factors that may affect image capture quality or image interpretation, including body position, head position, the use of assistive equipment, or other circumstances which may affect the quality, visibility or comparability of facial imagery. OIFR Users must not assume that a highly ranked or visually similar result is a Viable Match.<br>• Where a Viable Match is identified, any subsequent policing decision must be based upon the totality of available information and intelligence and not solely upon the OIFR result. The level of documentation required will be proportionate to the operational context and in accordance with the relevant OIFR operating procedures.<br>• A Viable Match constitutes an intelligence lead only and does not, in itself, amount to formal identification or evidential proof of identity. | | | |

| | | | | |
|---|---|---|---|---|
| | • For example, the system may present subjects who appear noticeably older or younger than the person depicted in the Probe Image. Such differences do not automatically render a match non-viable, but the OIFR User must assess whether the apparent age variation can be explained by natural ageing, the time lapse between images, or other relevant factors. Similarly, where disability, injury, medical treatment or assistive equipment may affect appearance or image quality, these factors must be considered as part of the overall assessment of whether a Potential Match may constitute a Viable Match.<br><br>• **Ongoing Testing,System Assurance and similarity score threshold:** The MPS undertakes ongoing system assurance and performance monitoring to ensure that OIFR continues to operate effectively, fairly and proportionately.<br>• The OIFR system incorporates a similarity score threshold designed to reduce the likelihood of irrelevant results being returned for user review. This threshold has been informed by testing and evaluation and is subject to ongoing monitoring and review. The threshold is currently set at 6600 (0.66) and forms an important safeguard in supporting the fair, accurate and proportionate operation of the OIFR System.<br>• By filtering lower-confidence results, the threshold helps reduce the risk of individuals being incorrectly identified and therefore mitigates the potential for adverse impacts arising from false matches. The threshold forms one element of the broader OIFR control framework and does not replace the requirement for | | | |

| | | | | |
|---|---|---|---|---|
| | human review and adjudication, including consideration of factors that may affect facial appearance, image quality or image interpretation.<br>• Any proposed amendments to the threshold are subject to governance, testing and assessment to ensure that system performance continues to support operational effectiveness whilst mitigating the risk of false matches and unintended impacts on individuals.<br><br>• **Training**: All OIFR Users are required to complete training before they are authorised to use the system.<br><br>• Training includes the legal and ethical framework governing OIFR, operational procedures, system limitations, human review and adjudication requirements, equality considerations and diversity awareness. Training also includes consideration of factors which may affect facial appearance, image quality and image interpretation, including the potential impacts of disability, injury, medical treatment, age progression and the use of assistive equipment. OIFR Users must maintain their competence in accordance with MPS training requirements.<br><br>• **Monitoring OIFR Viable Matches**<br>The MPS maintains records relating to OIFR Searches and outcomes to support governance, oversight, audit and compliance monitoring**.**<br><br>• Relevant information relating to searches, outcomes and demographic characteristics will be analysed to support ongoing assessment of operator | | | |

| | | | | |
|---|---|---|---|---|
| | performance, system performance, equality impacts and compliance with the Public Sector Equality Duty. This includes monitoring to identify any emerging disproportionality or unintended impacts affecting people who share protected characteristics, including disabled persons.<br><br>• **Post OIFR Search Monitoring**: OIFR usage, performance and governance information will be reviewed through regular reporting via the MO3 FR Team and the established MPS Facial Recognition Technology Board.<br><br>• Monitoring will consider operational use, compliance, equality impacts, performance trends and any emerging issues. Findings may inform changes to policy, operating procedures, training, governance arrangements or system configuration where appropriate. This includes consideration of any identified issues relating to image quality, accessibility, equality impacts or the operational use of OIFR involving persons with protected characteristics.<br><br>• **Transparency and Public Reporting:** The MPS is committed to transparency in its use of OIFR. Relevant policies, impact assessments and supporting governance documentation will be published on the MPS website to support public understanding of how OIFR is governed and used.<br><br>• Subject to technical feasibility, legal requirements and data availability, the MPS will publish information relating to OIFR use, performance and oversight through appropriate reporting mechanisms. The MPS will maintain a record of composition of (i) sex, (ii) race by IC Code and (iii) age range of OIFR | | | |

| | | | | |
|---|---|---|---|---|
| | searches. This may also include aggregated information relating to system use, outcomes, accessibility considerations and equality monitoring activities.<br>• The publication of governance and equality information supports public understanding of the safeguards applied to OIFR, including the role of human adjudication, the intelligence-led status of Viable Matches, Annex D approval requirements, accessibility measures and ongoing equality monitoring.<br><br>• Additionally, the MPS Facial Recognition Public Website shall cater for the visually impaired with accessibility to text-to-audio functionality. | | | |

| STEP 6. Ensure monitoring and review arrangements are put in place | GUIDANCE |
|---|---|

How will the implementation of the proposal / policy be monitored and by whom?

The MPS Facial Recognition Technology Board. This board meets on a regular basis. The Facial Recognition Technology Board is currently chaired by MPS Deputy Assistant Commissioner. This board is attended by a variety of key stakeholders and SME's from across the MPS and partners. The MPS Facial Recognition Technology Board will continue to take place to provide oversight and scrutiny for MPS OIFR use, discuss relevant issues arising from its use and public attitudes. They will also ensure continued compliance with the MPS OIFR Documents, Data Protection Act 2018 and the Equality Act 2010.

**All Public Authorities such as the Metropolitan Police Service (MPS) have to comply with section 149 of the Equality Act 2010 more commonly known as the General Duty.**

**The Duty requires us to:**

- **Eliminate discrimination, harassment and victimisation and any other conduct that is prohibited by or under the Act.**
- **Advance equality of opportunity between people who share a relevant protected characteristic and people who do not share it.**
- **Foster good relations between people who share a relevant protected characteristic and those who do not share it.**

**One of the ways we can demonstrate that we are complying with the General Duty is to document how decisions are reached and resulting activities including monitoring and review arrangements. In the MPS, the way we evidence this is by completing EIAs.**

What is the timetable for monitoring, with dates?

The Facial Recognition Technology Board meets on a quarterly basis, or such other frequency as may be deemed appropriate by the chair. This ensures that any actions raised can be met in a timely manner and any issues surrounding compliance can also dealt with expeditiously.

| STEP 7. Public availability of reports / result. What are the arrangements of publishing, where and by whom? | GUIDANCE |
|---|---|

In the interests of openness and transparency, this document will be available on both the MPS Facial Recognition external facing website and the internal intranet.

This Document is the copyright of MOPAC and my not be reproduced in whole or in part without the express written permission from MOPAC ©MOPAC 2012