DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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

1. Introduction

1.1 As a `public body', the Metropolitan Police Service (MPS) is subject to the requirements and conditions imposed by the European Convention of Human Rights (ECHR) and the Data Protection Act (DPA) 2018. The legislative requirements place an obligation on the MPS to process personal data fairly and lawfully in order to safeguard the rights and freedoms of individuals.

1.2 Article 35 of the General Data Protection Regulation (GDPR) and Section 57 of the DPA 2018, mandate the completion of a Data Protection Impact Assessment (DPIA) for organisations with technologies and processes that are likely to result in a high risk to the rights and freedoms of data subjects.

1.3 The DPIA process helps an organisation find and fix problems during the early stages of any project, helping to prevent breaches of data protection law and/or breaches of regulations for which very significant fines can be levied. For the MPS this also helps prevent damage to the trust and confidence of the public and other key stakeholders.

1.4 DPIAs also support the principle of accountability as they help organisations to comply with the requirements of the GDPR and the DPA 2018, and to demonstrate that appropriate measures have been taken to ensure compliance.

1.5 When completing a DPIA we must consider whether the project or initiative in question involves data sharing arrangements with a third party. GDPR Article 28(3) requires that data processing is governed by a contract that is binding on the processor with regard to the controller. The contract sets out the subject matter, duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller.

1.6 Advice issued by the Information Commissioner's Office (ICO) is that the DPIA process should commence during the very early stages of a project and most certainly before any data is processed. Work on the DPIA should run alongside the planning and development process.

Use of the MPS RFR DPIA

1.7 This document is designed to be used as an overarching DPIA to support the use of Retrospective Facial Recognition (RFR) by the MPS for:

(a) searching the Custody Images Dataset;

(b) searching the Unresolved Crime Cache[1]; and

(c) searching the Temporary Image Reference Library.

1.8 Future use-cases for the RFR System are likely to fall outside the nature and scope of the data processing contemplated by this DPIA for example where additional Substantive Image Reference Libraries are made available for searching. Accordingly those seeking to use RFR should **review** this DPIA. If the proposed data processing is not covered, or there are further

[1] RFR Searching of the Unresolved Crime Cache will not be available at the point the MVP RFR System is brought into operation. The DPO has been notified of this since the approval of this form and no concerns have been raised, noting that this lessens the extent of the data processing overall.

controls and/or safeguards to be added, the DPIA should be **amended** or supplemented with an annex, prior to **adoption** as a DPIA for that specific RFR use-case (**Use-case Specific DPIAs**). The need for any use-case Specific DPIAs should be considered with the MPS Data Protection Officer (**DPO**) when:

(a) A RFR Approving Officer is considering an MPS RFR Form 1 and/or MPS RFR Form 2 to approve an Image Reference Library; and/or

(b) a Probe Image is being considered for RFR Searching and it falls outside the scope of this DPIA and the associated MPS RFR Documents as drafted.

1.9 Adopted Use-case Specific DPIAs will contain similar wording across key areas with amendments made, additional annexures created where necessary to reflect any specific characteristics of an Image Reference Library, Probe Image or particular use case.

1.10 This document should be read in conjunction with the MPS RFR Documents.

Role of the Data Protection Officer

1.11 For those involved in the review, amendment (as necessary) and adoption of a DPIA especially in relation to the decisions to approve Image Reference Libraries and sensitive Probe Images, there is a need to engage with the Data Office before an amended DPIA is submitted to the DPO for sign-off. Their advice is crucial to ensuring that any proposals meet the requirements of the DPA 2018. As well as providing advice, the DPO is able to monitor compliance with the DPA 2018, and in doing so provides assurance to the Commissioner. The fact that the DPO is an independent body provides further assurance. The DPO's involvement in the approval of Image Reference Libraries and is engaged the Facial Recognition Strategic Board and is evidenced by their sign-off of the overarching DPIA for RFR and any amended DPIA to cater for specific RFR use-cases.

2. Data Protection and Data Processing

Purpose of the processing

Purpose of RFR

2.1 RFR technology is used by the MPS as an after-the-event capability to help officers establish who a person is or whether their image matches against other images held by policing in order to help progress investigations and operations. It is envisaged that the RFR System will primarily be used as a tool for the furtherance of investigation, rather than to shape live events, noting that there are certain circumstances where live events will be influenced e.g. where a match is made against a person currently in police custody or where operational circumstances demand that all tools are deployed. It helps officers work more efficiently and effectively to keep Londoners safe. Non exhaustive examples of how RFR technology may do this include:

(a) To aid investigations by providing a lead as to the potential identity of a subject, confirming where a subject appears within a set of imagery, or establish who a person is pictured as having been associated with;

(b) Use in the custody environment to help ensure the early flagging of risks to officers and ensuring links are made to others' investigations where the subject is also of interest to the police; and

(c) To aid the identification of the deceased, grievously injured or unresponsive including so as to assist with making timely contact with family members.

2.2 While it is the case that the MPS has access to the Police National Database (PND), which also has a facial matching function, the RFR System will fulfil a fundamentally different purpose, being directly available to operational policing (with RFR SPOCs embedded in units) and conducted against libraries which are more likely to be responsive to searches. The MPS RFR System will operate an Unresolved Crime Cache which will permit (time-limited) searching against new custody images. It also has enhanced technical capabilities such as facial image ingestion directly from video. The MPS's objectives for RFR are further outlined in the MPS RFR Documents, particularly in relation to the strategic, operational and technical objectives which may be found in the MPS RFR policy.

2.3 It is important to note that this DPIA relates to the "Minimum Viable Product" (**MVP**) deployment of the RFR System. The data protection measures described in this DPIA are accurate for the MVP deployment, but further work and development (including further functionality) will be deliver in the finalised RFR System. The finalised RFR System is expected to be delivered during winter 2023. The DPIA and RFR Documents will be reviewed at that point, taking account of any lessons from the operation of the MVP RFR System.

Benefits of RFR

2.4 Identified opportunities for RFR include:

- **Accelerating crime investigations** – RFR will be used to detect faces in video footage or images and match them against known faces within a reference database.
- **Developing targeted intelligence** by, for example, analysing media obtained from open source platforms that feature activities of gang members, subject to the usual controls around the extraction of personal data from social media (which would include issues around expectations of privacy).
- **Help mitigate an imminent threat to public safety** - such as following terrorism, and protecting the public through the disruption of those seeking to commit terrorist offences. In these circumstances, there is a need to swiftly and accurately review media to seek to promptly make identifications at a time of threat.
- **Finding missing persons** – e.g. police could submit a reference photo provided by a missing person's family and use RFR to search images obtained from relevant and intelligence led CCTV footage, noting that RFR is not intended to support real- time decision making, but to provide after-the-event intelligence leads.
- **Identify and find exploited children** – isolating the appearances of specific individuals in still images or moving media sequences can help accelerate the investigation of child exploitation cases.
- **Help to identify persons** who are unwilling to identify themselves or appear to be using someone else's identity or false identity where powers to take fingerprints are not available. As well as assisting in an investigative context, this is also relevant to policing in a protective security contact too.
- **Help identify a deceased person** or a person who is incapacitated or otherwise unable to identify themselves.
- **Protecting the custody environment** by assisting officers to make early identifications to facilitate the management of risk within custody and allow the MPS to check whether that person is wanted for other offences where the MPS has imagery linked to such offences.
- **Linking faces across different media**, even though no reference images are available. This will help with investigation of crimes happening repeatedly in the same location or in a number of locations but with the same method of operation.

RFR's benefits are further outlined in the MPS RFR Documents, particularly paragraph 1.9 of the MPS RFR Policy and Section 3 of the MPS RFR Legal Mandate.

Context of the processing

Relationship to individuals

2.5 RFR relates to individuals in three ways (1) those in a Probe Image (2) those in an Image Reference Library (3) protecting the public more generally.

2.6 **Probe Images**: A photograph of a person, where it is of a standard to use it as a Probe Image, represents that person's personal data. From it, that person could be recognised and it's taking and retention has been accepted to amount to an interference with Article 8.[2] The use of RFR to search against an Image Reference Library is also an act of interference with Article 8. The overall act of running a RFR Search:

(a) involves the creation of a biometric template of the person's facial features – this requires specific technical processing which is for the purpose of uniquely identifying an individual. This template comprises biometric data for the purposes of Section 205(1) of the DPA 2018. A greater level of sensitivity attaches to this type of data and this was recognised by the Court of Appeal in the context of LFR in the *Bridges* case[3]; and

(b) aims to find matches against the Probe Image from within an Image Reference Library. Such matches can be revelatory and provide intelligence leads for further investigative activity. Depending on the level of detail held by the police in relation to an individual, a match may help the police identify that person and/or link a person to previously frequented locations, their associates, and information held by the police about their policing record or their pattern of life.

2.7 **Image Reference Library:** Images of persons held on a dataset by policing comprise personal data. *Gaughran v United Kingdom* recognises that there is a sensitivity to a dataset over a disaggregated collection of images noting:[4]

> *"The building up of a database of such data from those convicted of offences provides a very useful and proven resource in the battle against crime by reason of the assistance it provides in identifying individuals. It is clear that the larger the database the greater the assistance it will provide. While a universal database would be of immense help in combatting crime, weighing the private rights of individuals against the good which would be achieved by such a universal system requires the striking of a fair balance. Experience has shown that those who have committed offences may go on to commit other offences. A state decision to draw the line at those convicted of a substantial category of offences is entirely rational and furthers the legitimate aim of countering crime so as to protect the lives and rights of others."*

2.8 The effect of Gaughran is to mean that, compared to an image in isolation, an image enrolled into an Image Reference Library and made available for RFR Searching can potentially say more (about the person in the image) to more people (i.e. the RFR Search users of the Image Reference Library). For this reason Article 8 is engaged by the retention and RFR Searching of an Image Reference Library. This now extends to custody images as,

[2] See for example, para 64 of *Gaughran v United Kingdom (13 February 2020, Application 42345/15)*

[3] See para 88 of the judgment.

[4] At para 44 of the judgment.

in Gaughran, the court recognised for the first time that the taking and retention of custody images amounts to an interference with Article 8.

2.9 In *Bridges,* in the context of live facial recognition, the court recognised two questions arose that conferred too greater a discretion on officers to determine policy on a case-by-case basis such that the overall use of live facial recognition in that specific case was found not to be foreseeable and therefore in accordance with law. These two questions where termed by the Court of Appeal to be the 'Who Question' and the 'Where Question' – in essence who could be placed on a LFR Watchlist for location and where LFR could be deployed to locate the people on an LFR Watchlist. A similar position exists for RFR especially when drawing on common law powers and the questions for the MPS are addressed by way of a published policy. This provides an answer such that the use of RFR by the MPS for its use-cases can be foreseen by the public. These points may be termed the 'What Question' and the 'How Question' and essentially go to the points where RFR results in inference with Article 8 Rights and involves sensitive data processing:

(a) The 'What Question' – this is a question as to the images which may be used for RFR Searching and what controls, safeguards and approvals attach to them? The MPS RFR Documents answer this by:

(i) placing controls and safeguards around the selection and use of Probe Images for RFR Searching including the adoption of a tiered approach to the selection of Probe Images that focuses consideration on the sources of Probe Images and the expectations of privacy that attach to such images;

(ii) outlining the process by which approved Image Reference Libraries may be searched. The controls and safeguards are designed to recognise that different Image Reference Libraries have differing levels of sensitivity and it is necessary to ensure undue data processing is minimised when a less intrusive Image Reference Library would allow the policing objective to be achieved. Accordingly the MPS RFR Documents implement a staged process to RFR Searching outlining an approval process to approve an Image Reference Library as being eligible for RFR Searching both in relation to Substantive Image Reference Libraries with ongoing utility to the MPS and Temporary Image Reference Libraries of relevant to a specific investigation or operation;

(iii) implementing specific controls and safeguards in relation to certain protected characteristics – including where a risk of exploitation may otherwise arise;

(iv) providing direction to both those being asked to approve the use of an Image Reference Library for RFR Searching and those undertaking RFR Searching in terms of how Image Reference Libraries may be approached in terms of the intrusion and data processing that attaches to them and when elevated privacy considerations may arise; and

(v) detailing when images may be selected for ongoing RFR Searching against holdings against the MPS' Image Reference Libraries and the further controls and safeguards which attach to this process.

(b) The 'How Question' – this is a question as to how an RFR Search should be undertaken including how officer decision making is channelled to ensure safeguards are in place to undertake a proportionate search, targeted on need as opposed to facilitating a 'search all' approach or allowing undue levels of discretion. The MPS RFR Documents answer this by:

(i) outlining the purpose and specific grounds for when an RFR Search may be undertaken – this approach limits undue discretion and ensures that searches have a policing objective;
(ii) detailing the pre-requisites to undertake an RFR Search to ensure less intrusive options have been considered and that a necessity case to act is made out;
(iii) specifying the process to undertake an RFR Search and the approvals that attach to RFR Searching; and
(iv) detailing the role of the human-in-the-loop during the Adjudication process and ensuring the nature of RFR Search results are disseminated as part of any results.

2.10 Public protection: RFR has the potential to engage the wider public, not least in the context of using imagery from a public space for RFR analysis and the impact this may have on public perception and attendance at a location. The effective use of RFR to progress operations and investigations by the MPS serves wider public protection and safeguarding purposes. There is therefore a substantial public interest in enabling the MPS to use RFR to accelerate crime investigation, improve justice outcomes, locate missing persons, and effectively link information and intelligence in line with its law enforcement purposes.

2.11 **Data Protection Impact Assessment and Image Reference Libraries:** as noted in paragraph 1.8, each Substantive Image Reference Library or Temporary Image Reference Library that is added to the RFR System for searching will be considered by the DPO, with the need for a Use-case Specific DPIAs evaluated at the time.

Custody Images Dataset

2.12 The initial Image Reference Library that will consist of images obtained from the MPS's custody images system and in this DPIA it is referred to as the **Custody Images Dataset** in this DPIA. The Custody Images Dataset has/will have the following characteristics:

(a) It consists of consists of 999,334 images of people detained in police custody by the MPS. The individual images that make up the Custody Images Dataset were captured using police powers set out in S.64A of the Police and Criminal Evidence Act 1984 (PACE).

(b) The Custody Images Dataset does not contain all of the images held by the MPS. The images imported from the general custody images holdings are filtered by reference to Management of Policing Information (MOPI) group offence and age of data subject as an additional safeguard, noting the additional processing RFR entails:

(i) For MOPI Group 1 and 2 offences, only images which are 10 or less years old will be uploaded in to the Custody Images Dataset.
(ii) For MOPI Group 3 offences, only images which are 6 or less years old will be uploaded to the Custody Images Dataset.

(iii) In relation to data subjects who were under the age of 18 when they had their image taken:

(A) Images of children under the age of 13 have not been included in the Custody Images Dataset.

(B) For children aged 13 – 15, images have only been included where the underlying criminal offence which led to the arrest was in the MOPI Group 1 or 2 categories, subject to the issue set out paragraph 2.37.

(C) For children aged 16-18 arrested for MOPI Group 3 offences, it has been determined that there is some benefit in keeping track of offending at this age, but in order to avoid being disproportionate, it would be appropriate to only retain these images for 3 years.

(c) The currency of the Custody Images Dataset automatically through a 'delta link' to the MPS's custody images system. The 'delta link' ensures that images deleted from the MPS custody image system are automatically deleted from the Custody Images Dataset and that new images added to the system are also added to the Custody Images Dataset.

2.13 The MPS holdings of custody images comes from two systems. The historic CSIS/CIS system and the current CONNECT system.

2.14 A known issue exists in relation to data subjects linked to images taken in relation to MOPI 3 offences in the CONNECT system. As a result of technical issues it has proved impossible to disaggregate the MOPI 3 images from the MOPI 1 & 2 image. This is referred to as the **U16 MOPI 3 CONNECT Cohort Issue** and is considered in detail below.

Temporary Image Reference Library

2.15 A Temporary Image Reference Library is created for a discrete purpose linked to a specific investigation or operation. Such libraries may see images collated by the MPS including following a public appeal or another investigatory technique. The management and retention of image collections is a distinct undertaking from any RFR Searching against an ingested Image Reference Library and accordingly falls outside the scope of this policy.

2.16 Unlike Substantive Image Reference Libraries, Temporary Image Reference Libraries are not available beyond a relatively small number of people involved in a specific investigation or operation. A Temporary Image Reference Library does not meet an ongoing policing requirement generally but is time-limited to meet the needs arising from a specific investigation or operation. Accordingly the privacy considerations, scope and scale of any potential use and safeguards needed are different and relate to a specific operational policing use-case.

2.17 It is anticipated that Temporary Image Reference Libraries falling within the parameters set out above will not require a Use-case Specific DPIAs.

Technology

2.18 It is important that any facial recognition tool is considered in terms of statistical accuracy and accuracy in the context of different demographics. A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result the MPS has paid regard

to the evaluations undertaken by the National Institute of Standards and Technology (NIST) and the research undertaken by the National Physical Laboratory (NPL).

2.19 To assist the public and users of the RFR System with understanding how the MPS meets its PSED duties, the MPS has published the MPS RFR Equality Impact Assessment. Additionally, the MPS has published a paper entitled 'Understanding the Metropolitan Police Service RFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to understand the statistical accuracy and demographic performance of its RFR algorithm. This includes:

(a) **Independent evaluation:** A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result the MPS has paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by the MPS.

(b) The NPL has also undertaken specific operational testing of the MPS RFR system, the outcome of which is reflected in the paper referred to above. The NPL testing showed that the RFR System was 100% statistically accurate.

(c) **Peer review:** The MPS's position paper has been reviewed by other experts in the field including the Defence Science and Technology Laboratory and the National Physical Laboratory.

(d) **Ongoing assurance:** The MPS RFR Documents provide for ongoing evaluation and a review process. This reflects the ongoing nature of the PSED duty and also offers the MPS a chance to monitor for technical issues by reviewing performance and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS Facial Recognition Strategic Board.

(e) **Monitoring data:** will provide a breakdown of demographic details and RFR User information, so as to enable the FRT Board to exercise an oversight function.

2.20 The MPS RFR Documents also provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing need to understand the performance of an algorithm, particularly in operational contexts and also offers the MPS a chance to monitor for technical issues by reviewing all RFR results and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS Facial Recognition Strategic Board.

Public perception and expectations

2.21 **MOPAC Public Attitudes Survey**: concluded that the MPS's use of innovative technology is high, but varies by age, ethnicity and broader attitudes towards the police. In Q4 FY 22-23, approx. 3,800 Londoners were asked to what extent they support or oppose the MPS using technological innovations in a range of situations. It reported:

		New/innovative tech		Facial recognition tech		
		Solve crime	**UK borders**	**Violent/ serious offenders**	**Wanted by courts**	**At risk**
MPS		84%	85%	82%	82%	83%
Age	**65+**	89%	92%	88%	90%	88%
Ethnicity	**White**	83%	86%	80%	81%	81%
	Mixed	74%	75%	72%	73%	71%
	Asian	88%	91%	87%	88%	88%
	Black	75%	82%	75%	80%	81%

The role of the Information Commissioner and Biometrics' Commissioner

2.22 Whilst the MPS would welcome and wish to be part of any process to produce a code of conduct for the use of RFR, having regard to our track-record of responsiveness to the views expressed by the commissioners. The MPS has paid regard to the ICO and the opinion issued by the Information Commissioner in relation to facial recognition technologies (especially in relation to LFR).

Nature of the processing

Data overview

A.	SUMMARY OF PARTICIPANT PERSONAL DATA TO BE CONTROLLED BY THE DATA CONTOLLER - MPS				
	PURPOSE: To enable the MPS to use RFR Systems in furtherance of its law enforcement purposes.				
Ser.	**Personal Data Captured**	**Whose data is processed**	**Who has access to the Personal Data**	**Why the Personal Data is needed**	**How long is the Personal Data retained for**
Personal Data: [5]					
1.	Facial image	Subject(s) in image	MPS personnel based on the role and need to access imagery.	RFR, ADJ, SAFE, FIO, SD, DPA	Matched facial images are retained as part of the investigation in accordance with MOPI RRD requirements. Non-matching images are not retained.
May be derived from the image					
2.	Perceived gender	Subject(s) linked to image	MPS personnel based on the role and need to access data.	ADJ, SAFE, FIO, SD, DPA	In accordance with relevant MOPI period.
May be associated with the image (by reference to other indices controlled or accessible to the police):					
3.	Name and on occasion, description of subject	Subject(s) linked to image	MPS personnel based on the role and need to access data.	ADJ, SAFE, FIO, SD, DPA	In accordance with relevant MOPI period.
4.	Unique Reference Numbers (for example PNC ID number, CRO number)				In accordance with relevant MOPI period.
5.	Contact details including address and phone number				In accordance with relevant MOPI period.
6.	Date of birth				In accordance with relevant MOPI period.
7.	Recorded gender				In accordance with relevant MOPI period.
8.	Metadata (including location and time image was taken)				In accordance with relevant MOPI period.
Special Category Data / Sensitive Processing: [6]					
9.	Biometric facial template (of those in a Probe Image and on Image Reference Libraries searched against)	Subject(s) in image	MPS personnel undertaking searching, management of the RFR system and responsible for DPA requests.	RFR, ADJ, SAFE, FIO, SD, DPA	Biometric template of Probe Image will be retained in the system for a period of 3, 6 or 9 months (depending on MOPI Group), the User will then be prompted to review (for example where the crime is unresolved) or delete the template. Templates held in the Custody Images Dataset will be held for a period not exceeding 10 years (for

[5] Means any information relating to an identified or identifiable **living** individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only be potentially linked to a living individual.
[6] Means the processing of personal data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, (ii) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual, (iii) the processing of data concerning health, (iv) the processing of data concerning an individual's sex life or sexual orientation.

					MOPI Groups 1 and 2), 6 years (MOPI Group 3) or 3 years (MOPI Group 3 where detainee is under 18.
May be derived from the image					
10.	Perceived ethnicity	Subject(s) linked to image	MPS personnel based on the role and need to access data.	ADJ, SAFE, FIO, SD, DPA	In accordance with relevant MOPI period.
11.	Perceived beliefs (for example, clothing with religious significance).				In accordance with relevant MOPI period.
May be associated with the image (by reference to other indices controlled or accessible to the police):					
12.	Recorded ethnicity	Subject(s) linked to image	MPS personnel based on the role and need to access data.	ADJ, SAFE, FIO, SD, DPA	In accordance with relevant MOPI period.
13.	Availability of other biometric modalities (DNA, fingerprints)				In accordance with relevant MOPI period.
14.	Warning markers associated with the subject (for example, possession of weapons, drugs, ailments, firearms, mental health, violence).				In accordance with relevant MOPI period.
15.	Criminal record data (both in relation to previous offences and any current investigation or operation).				In accordance with relevant MOPI period.

Key:			
Purpose of which personal data is processed			
RFR	To run the RFR search	**ADJ**	To undertake Adjudication in relation to a Potential Match
SAFE	To discharge safeguarding responsibilities complimentary to a law enforcement purpose – for example in relation to police and detainee safety in a custody context.	**FIO**	To further an investigation or operation in line with a law enforcement purpose
SD	To generate statistical data and undertake research as regards system performance for assurance.	**DPA**	For the purposes of providing oversight and managing the processing of personal data particular where a need arises to consider Right of Access Requests and Freedom of Information Act 2000 requests.

B. RETENTION RATIONALE: FOR PERSONAL DATA UNDER MPS CONTROLLERSHIP

Data Types	Retention Period	Rationale for Retention Period
Serials 1	Relevant MOPI period	Although not evidential it is considered necessary for the OIC to be able to show the process through which the lead was generated, therefore the match report showing the Probe Image and the Library Images will be retained in PDF format (not templated).
Serials 2 to 8 and 10 to 15	Relevant MOPI period	This data will be retained in accordance with the relevant MOPI policy in the normal course of business.
Serial 9	3, 6 or 9 months (depending on Tier, as defined in the RFR Policy),	The templated image will be retained unless actively deleted by the User for a period 3, 6 or 9 months (dependent on Tier), at which point the User will be prompted to delete or extend the period of retention for the template. A user would be expected to extend the life of the template in circumstances where the relevant investigation was ongoing and it is appropriate for the template to remain in the Unresolved Crime Cache.

Nature of the processing

The data created by the RFR system

2.23 **Biometric Data**: RFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to make possible matches against persons of interest to the MPS. Where the RFR system identifies a Potential Match the RFR System returns these to a trained member of MPS personnel who then makes a decision as to whether the Potential Match is a Viable Match. The RFR system therefore creates biometric data in two ways:

(a) the Templating of Probe Images produces personal biometric data; and

(b) the Templating of images on Image Reference Libraries being searched against Probe Images also produces personal biometric data.

Sources of data used during the RFR process

2.24 The MPS RFR Policy outlines and provides a means to assess the sources of Probe Images (in relation to Probe Image Levels) and the purpose for which Probe Images can be used. The MPS RFR Policy Document also outlines and provides a means to assess sources of Image Reference Libraries (in relation to Image Reference Library "Levels" describing different levels of intrusiveness). As well as MPS data such as custody images, EWMS, PNC and operation/investigation specific sources, data may be provided by other police forces and agencies associated with law enforcement as well as the wider public as they would more generally to assist the MPS with its law enforcement duties. This would be particularly relevant, for example, in relation to missing persons where the image and other data may be provided by that person's family or CCTV which provides footage of a crime where the majority of CCTV is not controlled by, but shared to the police.

Data storage and review

2.25 **Data storage on the RFR system:** The RFR system is hosted in a secure MPS-owned operating environment. The RFR system has been subject to rigorous security testing.

2.26 **Importing Image Reference Libraries onto the RFR system:** Image Reference Libraries are ingested into the system from within the secure MPS operating environment.

2.27 **Data storage on wider MPS systems:** The data is held securely on MPS systems accessible via the MPS computer system, Aware. Officers leaving the MPS automatically have their account disabled and therefore would no longer have access to the information. The MPS has its own policy on retention, review and disposal that applies to this information, including the need to hold and review policing information in accordance with MOPI and CPIA (as applicable).

Data retention

2.28 With regards to data retention, the MPS RFR Documents provide that:

(a) Where the RFR system does not generate a Potential Match, then a person's biometric data and Probe Image is marked for deletion from the RFR System unless the biometric template and facial image is retained as part of the Unresolved Crime Cache for ongoing searching in line with approval attached to that image. The biometric template and Probe Image will be deleted as soon as practicable following:

(i) a Viable Match meaning the data no longer needs to be in the Unresolved Crime Cache;
(ii) the expiry of the relevant Tier period (as specified in the RFR Policy) where the Probe Image has been designated for inclusion on the Unresolved Crime Cache; or
(iii) the investigation being otherwise resolved.

(b) Where the Probe Image is designated for inclusion within the Unresolved Crime Cache for a period of the image will be held in that cache for period dependent on the gravity of the offence. Personnel will be required to review Probe Images in the Unresolved Crime Cache every 3 months for Tier 3 offences (least serious offences), 6 months for Tier 2 and 9 months for Tier 1 (most serious) after designation for inclusion in the cache, to ensure the continuing need for the RFR Search. The Tiers are set out in Annex C of the MPS RFR Policy and have themselves been subject to a DPIA assessment as part of the FIMS facial library DPIA.

(c) Where the RFR system generates a Potential Match all personal data associated with a Probe Image is deleted as soon as practicable and in any case within 31 days except where:

(i) the Potential Match is confirmed as a Viable Match and then personal data is retained in accordance with the DPA 2018 and MOPI; and/or
(ii) personal data is retained in accordance with the MPS's complaints / conduct investigation policies.

(d) In relation to Image Reference Libraries, these are not dedicated resources linked to RFR and will be retained by the MPS in line with the policy applicable to them (save that in some cases additional safeguards may be put in place to ensure proportionality) via a 'delta link'. From an RFR perspective, they will cease to be available for RFR Searching and deleted from any RFR system on expiry of any approval to use the Image Reference Library for RFR Searching. Images imported via the 'delta link' to an Image Reference Library will cease to be available for RFR Searching 'by design' if the underlying image is deleted.

Data retention and the Custody Images Dataset

2.29 Custody images are subject to the rules set out in the MOPI policy which set out the basis on which the police may retain information. MOPI classifies all offences under one of three headings: MOPI Group 1 (serious offences and public protection matters); MOPI Group 2 (other sexual and violent offences); and MOPI Group 3 (all other offences). MOPI Group 1 data can be retained for up to 100 years, with a review after 10 clear years to ensure adequacy and necessity. MOPI Group 2 are subject to a 10 clear year review period. MOPI Group 3 are subject to review at 6 clear years. New images from the custody image system

are imported into the Custody Image Dataset. Where an image has been deleted from the MPS custody image system the corresponding deletion is made to the Custody Images Dataset.

2.30 As an additional safeguard, noting the heightened intensity of the processing, the MPS has applied stricter rules to the operation of the Custody Images Dataset than are required by MOPI. The Custody Images Dataset is configured to ensure that offences under MOPI Groups 1 and 2 are automatically deleted 10 years from the date of capture fully using the initial MOPI period, with no additional period added to anticipate any possible extension. . No provision is made in the Custody Images Dataset for the possibility that a review would authorise the retention of an image. MOPI Group 3 images in the Custody Images Dataset are no older than six years from the date of capture, aligning with MOPI 3 requirement for review or deletion at that point.

2.31 **Age considerations.** The Custody Images Dataset includes additional safeguards:

(a) Under 13s have the highest expectation of privacy, and the MPS has also paid regard to the prospects of gaining results from this capability. Images of children under the age of 13 have not been included in the Custody Images Dataset.

(b) For children aged 13 – 15, images have only been included where the underlying criminal offence which led to the arrest was in the MOPI Group 1 or 2 categories. The policing benefit of including MOPI Group 3 offences is considered marginal and in the context of expectations of privacy may risk, all else being equal, being disproportionate as a default approach based on the current crime challenges. This is subject to the U16 MOPI 3 CONNECT Cohort Issue.

(c) For children aged 16-18 arrested for MOPI Group 3 offences, it has been determined that there is some benefit in keeping track of offending at this age, but in order to avoid being disproportionate, it would be appropriate to only retain these images for three years.

Data sharing

2.32 Should the RFR system generate a Potential Match, the subsequent process would typically also involve MPS personnel using policing databases and other intelligence systems as part of the Adjudication process and to inform any further action. This subsequent action may also involve the MPS working with other police forces, law enforcement bodies, and other agencies to assist the MPS in discharging its common law policing powers. This action will not require the sharing of biometric data but may require the MPS to share personal data, as it would for any investigation, in accordance with the MPS's routine sharing arrangements.

High risk processing

2.33 **Innovative Technology**: RFR is not a new technology to law enforcement. Unlike other applications for facial recognition, RFR technology has been used for over a decade by law enforcement.

2.34 **Biometric Data**: The RFR system processes biometric data, both in relation to Probe Images and Image Reference Libraries. Security measures including safeguards 'by design' have

been identified and implemented in this DPIA and the MPS RFR Documents to mitigate risk in relation to biometric data processing.

2.35 **Data Matching**: RFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify possible matches against persons of interest to LEAs. The Adjudication process requiring human-in-the-loop decision making, and other mitigants have been identified and implemented in this DPIA and the MPS RFR Documents.

2.36 This DPIA identifies the safeguards put in place in relation to potential high risk processing activities. The MPS is content that the residual risk in relation to the data processing is mitigated by the MPS RFR Documents and this DPIA and is not considered to be high risk as a result.

2.37 **U16 MOPI 3 CONNECT Cohort Issue:** It has become apparent that as a result of technical issues it has proved impossible to disaggregate the MOPI Group 3 images from the MOPI Groups 1 & 2 images in the CONNECT system within the 13-15 age range. The intention had been to exclude the images associated with those data subjects arrested for offences falling within MOPI Group 3 (which is the least serious group of offences). Although it is impossible to determine the actual numbers of data subjects falling within MOPI Group 3 without undertaking a manual sift of the 2066 data subjects in the CONNECT 13-15 cohort , if the 13-15 CONNECT cohort mirrors the breakdown of the CSIS/CIS figures, then it may be assumed that at the point the RFR System goes live, that c.520 data subjects are included in the system as a result of the U16 MOPI 3 CONNECT Cohort Issue which would otherwise be excluded were the system working as intended. This number will grow as CONNECT increases in numbers.

2.38 Senior officers have considered two options in addressing the 13-15 CONNECT Cohort Issues: (1) exclude all of the data for data subjects aged 13-15 (in MOPI Groups 1, 2 and 3) pending a technical fix to CONNECT which would allow the disaggregation or (2) include all of the data aged 13-15, including those data subjects who were arrested for MOPI Group 3 offences, pending the necessary technical fix. The technical fix is anticipated to occur in November 2023. No form of manual weeding could remove the MOPI Group 3 data subjects from the RFR System and still allow the 'delta link' to operate automatically. At the point the fix is implemented the MOPI Group 3 13-15 CONNECT cohort will be automatically purged from the Custody Image Dataset.

2.39 Taking account of the very considerable policing benefit that the system offers and the prevalence of crime in that age group (and the extent to which victims of crime also fall within that age group), the seriousness of the crime data subjects in MOPI Groups 1 and 2 may be involved with, the difficulty justifying from a fairness perspective the exclusion of all MOPI Groups in the CONNECT system but permitting the inclusion of MOPI Groups 1 and 2 for CSIS/CIS, the relatively small numbers of data subjects impacted by the technical issue, the underlying lawfulness of the processing, and the relatively short period for which the additional intrusion will occur, senior officers have decided to permit the ingestion of entirety of the entire 13-15 CONNECT cohort (including the MOPI Group 3 data subjects) pending the implementation of the technical fix. This decision has been taken on the basis of the pressing social need, the limited impact on the proportionality of the processing, and the in-built assurance provided by there is a human-in-the-loop making the Adjudication, ensuring no automatic outcome.

Scope of the processing

Nature of the data

2.40 RFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to make possible matches against persons of interest to the MPS Where the RFR system identifies a Potential Match the RFR System returns these to a trained member of MPS personnel who then makes a decision as to whether the Potential Match if a Viable Match. The RFR system therefore creates biometric data in two ways:

(a) the Templating of Probe Images produces personal biometric data; and

(b) the Templating of images on Image Reference Libraries being searched against Probe Images also produces personal biometric data.

Level, frequency of data being processed and the individuals impacted

2.41 The below table summarises the key points during an RFR Search and the level, frequency, and nature of the data being processed. It also identifies those whose data is processed.

Level of data being processed	Probe Images	Unresolved Crime Cache	Image Reference Library	Adjudication
Biometric Processing	**Yes**	**Yes**	**Yes**	**Generally, no.**
	Biometric Templates are created for Probe Images.	Biometric Templates are created for Probe Images.	Biometric Templates are created for those on an Image Reference Library	The RFR system has generated Potential Matches for review. Further biometric processing will not be required, but other biometric modalities may on occasion be used to verify a person's identity where they are available. This

				is beyond the RFR process.
Imagery	**Yes**	**Yes**	**Yes**	**Yes**
	The Probe Image is submitted to the RFR system for templating.	Where no match against the Probe Image is submitted to the RFR system for templating and held in the Unresolved Crime Cache.	Images in the Image Reference Library are submitted to the RFR system for templating.	The facial images of Potential Matches are considered by the human-in-the-loop decision maker to determine the validity of any match.
Criminal convictions data	**No**	**No**	**No**	**Yes**
	The RFR system does not require this data to generate Potential Matches.	The RFR system does not require this data to generate Potential Matches.	The RFR system does not require this data to generate Potential Matches.	Personal data may be obtained - based on a policing need to undertake an Adjudication.
Personal data (such as name, date of birth, address)	**Yes**	**Yes**	**Yes**	**No**
	To the extent it is known, such data would be associated with a Probe Image	To the extent it is known, such data would be associated with a Probe Image	To the extent it is known, such data would be associated with an image in an Image Reference Library	No adjudication would take place on the basis of the biographic details (names etc), only as a result of Potential Matches determined by the RFR System.
Metadata	**Yes**	**Yes**	**Yes**	**Yes**
	In relation to Probe Images	In relation to Probe Images moved to the Unresolved Crime Cache	In relation to images in an Image Reference Library	In relation to Potential Matches to the extent it informs the Adjudication process.

2.42 Data is processed in relation to a specific RFR Search, the frequency of RFR Searches being based on the policing investigation or operation causing it to be necessary and proportionate to use RFR in furtherance of the MPS's policing powers.

2.43 The number of people falling within a RFR Search will vary by the design of the RFR Search. The MPS RFR Policy provide for a structured approach to searching in order to achieve a law enforcement purpose. It is based on (i) relevancy, (ii) expectations privacy and (iii) urgency. This avoids a 'search all' approach where a more tailored search is possible. Additionally in relation to Probe Images the following points also apply:

(a) the RFR System is designed to minimise collateral intrusion and unnecessary data processing that would fall outside of the 'explicit' processing criteria, for example by requiring manual verification of images for upload when an image with a number of faces in provided for ingestion into the system;

(b) where Probe Images Collections are proposed for searching, the MPS RFR Policy Document provides for a triaged approach to ensure the image most relevant to policing need are submitted for RFR Searching.

Geographical scope

2.44 RFR will be used across the geographic scope of the Metropolitan Policing District for the MPS law enforcement purposes. Whilst RFR may be used in relation to the MPS policing need which spans across London and reflects its role at a national level. Where locations of imagery raise elevated privacy concerns, the MPS Policy Document provide details to recognise these and provides a structured decision making and approval process to ensure the necessity and proportionality to use such images is fully made out.

3. Privacy Impact Screening Questions

Note: *Further advice regarding the screening questions can be obtained via the ISSU.*

		Yes	No
Q.1	**Will the project involve systematic and extensive profiling or automated decision-making to make significant decisions about people?**		X
Guidance	*Systematic monitoring is something that is targeted at broad categories of people rather than specific individuals. It is pre-arranged, organised or methodical, and is carried out as part of a strategy or general plan. Significant decisions may be those which affect entitlement to employment rights such as pay, pensions and*		

	allowances, deletion dates for cautions and other criminal records, decisions whether or not to investigate or treat someone as a suspect, or to contact them about their Engagement with the police.		
Answer	RFR is only triggered by a specific decision to submit a RFR Probe Image(s) for RFR Searching. The RFR Search is not triggered by automated decision making and all results are subject to a human-in-the-loop review.		
Q.2	**Will the project involve large scale use of special category data or criminal offence data?**	X	
Guidance	*The meaning of large scale is not defined in the Data Protection Act 2018. Factors to consider are the number of individuals whose data will be processed, the variety of different types of data, the volume of data, the duration of the processing, and the geographical extent of the data*		
Answer	Each search of a facial image involves the processing of personal biometric data in the creation and comparison of facial image Templates. A Template is a digital representation of the features of the face that have been extracted from the facial image. It is these Templates (and not the images themselves) that are used by the RFR system.		
Q.3	**Will there be systematic monitoring or profiling on a large scale, or in a public place?**	X	
Guidance	*This would include but is not limited to data captured from surveillance such as CCTV or facial recognition, and ticketing data from events or transport systems.*		
Answer	RFR is only triggered by a specific decision to submit a RFR Probe Image(s) for RFR Searching. There are however occasions where the Probe Image(s) may be at scale or the Image Reference Libraries used contain a larger data set such as CCTV over a period of time.		
Q.4	**Will the project be using new technology, or novel use of existing technologies?**		X
Guidance	*This will include cases where technology is used in a way which will result in a materially different outcome from the current way of processing data. Consider whether the technology will result in more people being identified, more types of data being captured, data about more people being used, or a larger number of people having access to the data. This is not intended to capture cases simply when a software package is upgraded to a newer version, unless the upgrade will itself produce significantly different results, for example, more thorough evidence review tools.*		

Answer	RFR is an established law enforcement capability with over a decade of policing use.		
Q.5	**Does the project do anything with DNA samples, DNA profiles and fingerprints?**		X
Guidance	*This includes doing anything with DNA samples, DNA profiles and fingerprints.*		
Answer	Whilst RFR does not involve DNA samples, DNA profiles and/or fingerprints, they may be part of the Adjudication process beyond the RFR Search and the RFR system does involve biometric processing in relation to people's facial features.		
Q.6	**Will the project combine, compare or match data from multiple sources?**	X	
Guidance	*This includes discussing individuals at multi-agency panels, as well as using databases and intelligence systems to collate information or wash data-sets against one another. It also includes processing following receipt of data from third parties.*		
Answer	Whilst Probe Images may come from a number of sources, all images must be lawfully held by the MPS with Probe Images being used to compare biometric templates against Image Reference Libraries. The decision to undertake an RFR Search, Adjudication and any consequential action may include the use of policing databases and other intelligence systems.		
Q.7	**Will the project process personal data in a way that involves tracking individuals' online or offline location or behaviour?**	X	
Guidance	*This would not extend to individual targeted surveillance authorisations.*		
Answer	The MPS RFR system is a closed system which does not involve the tracking of an individual's online or offline location or behaviour. It also does not provide an active monitoring capability as it analyses events retrospectively. It does however provides a result or a series of results based on previous events which may include how a person appeared and/or moved in a series of images.		
Q.8	**Will the project process personal data that could result in a risk of physical harm in the event of a security breach?**	X	
Guidance	*This would not extend to individual targeted surveillance authorisations.*		

Answer	*Putting security measures in place does not obviate the need to take this risk into account. The risk should be considered in the context of a breach.* Whilst security measures are in place to guard against security breaches, the RFR system involves the processing of biometric data and police data. Both categories are further considered below: Biometric data is recognised by the DPA 2018 as falling within the ambit of sensitive processing. Unlike a security breach relating to password data, the effects of a biometric data breach would be longer lasting making people more vulnerable to the consequences of a data breach, should the data be exploited. Police data can be highly sensitive. Its release could compromise the ability of the MPS to prevent and detect crime, and thwart the criminal justice system. Depending on the nature of the information, it may put people at risk were it to be known that they were of interest to the MPS.		
Q.9	**Will the project use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?**		X
Answer	Whilst the RFR system does involve the use of sensitive processing and biometric data, it does not involve the access to a service, opportunity or benefit.		
Q.10	**Will the project carry out profiling on a large scale?**	X	
Guidance	*The meaning of large scale is not defined in the Data Protection Act 2018. But this may include activities, such as using existing data to identify individual for operational purpose(s) or review.*		
Answer	The Probe Images searched and Image Reference Libraries compared against will be determined by the policing need. It is possible some more data intensive applications (e.g. batched searching of Probe Images Collections) would involve large scale processing.		
Q.11	**Will this project process personal data without providing a privacy notice directly to the individual?**	X	
Guidance	*You should consider any real-time interactions with individuals.*		
Answer	The provision of individual privacy notice personally to each person subject to an RFR Search would be impractical and detrimental to the policing purpose of undertaking an RFR Search. It would offer criminals an opportunity to exploit the information policing held or did not hold on them.		

Q.12	**Will the project process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?**	X	
Guidance	*The Data Protection Act 2018 places additional importance on the handling of children's personal data. You should consider any real-time interactions with children.*		
Answer	The RFR system processes all detected faces regardless of age but the MPS RFR Document provide for controls and confirm the diligence undertaken in relation to the RFR system and age.		
Q.13	**Will the project carry out any of the following:** • **Evaluation or scoring?** • **Automated decision-making with significant effects?** • **Systematic monitoring?** • **Processing of sensitive data or data of a highly personal nature?** • **Processing on a large scale?**	X	
Answer	The system creates an individual biometric Template for each face detected and compares that to the image Reference Library image.		

4. Data Protection and 'Privacy Law' Assessment

<u>European Convention of Human Rights</u>
Article 8 - Right to respect for private and family life:-

Everyone has the right to respect for their private and family life, their home and their correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Legality

2.45 The MPS RFR Legal Mandate for the use of RFR provides detailed analysis relating to Article 8 and other legal considerations relevant to the use of RFR. In relation to the Custody Image Dataset, the legal basis for the processing is set out in Section 2.3(a) of the RFR Legal Mandate.

Accountability

2.46 The MPS has developed a governance structure with the engagement of key stakeholders, to deliver accountability. This is covered within the MPS RFR Documents.

Home Office Biometric Strategy Published June 2018

2.47 The strategy sets out how the Home Office and its partners currently use biometric data, and their approach to future developments. The MPS has sought and obtained inclusion within the National Biometrics Oversight and Advisory Board as mentioned in Chapter 3 of the Strategy.

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

Does this project / initiative address a pressing social need? If so, outline it here:

2.48 Key powers the MPS may rely on when utilising RFR technology include the common law policing powers to:

- protect life and property;
- preserve order and prevent threats to public security;
- prevent and detect crime;
- bring offenders to justice;
- uphold national security.

2.49 Article 8 recognises action in the interests of national security, public safety, the prevention of disorder or crime as legitimate aims. The use of RFR in line with the MPS RFR Documents will help the MPS to achieve its law enforcement purposes.

2.50 Applied to RFR, the pressing social need is met on the following basis:

(a) **Accelerating crime investigations** – RFR will be used to detect faces in video footage or images and match them against known faces within a reference database in a way that is faster than it otherwise possible without compromising on human in the loop decision making. It is in the public interest that investigations are processed as expeditiously as possible. Specifically this enables:

(i) **Earlier management of public safety risk –** through the prompt identification, investigation and arrest of suspects – this is particularly relevant where there is an imminent threat to public safety where the public interest is served by disrupting those seeking to commit offences;

(ii) **Better outcomes** – being able to progress investigations more expeditiously increases the chances of being able to secure evidence. This helps facilitate the effective administration of justice which is in the public interest in terms of upholding the law and protecting society from those who break it;

(iii) **More effective use of resources** – as one of the largest employers in London and the South East of England, it is critical we use our resources most effectively to ensure we protect Londoners but also as tax-payers deliver a value for money service.

(b) **Finding missing persons** – e.g. police could submit a reference photo provided by a missing person's family and use RFR to search images obtained from relevant and intelligence led CCTV footage. In these types of difficult investigations, time matters and accordingly they can be resource intensive. It is in the public interest to effectively use technology to seek to safeguard those reported as missing as soon as possible.

(c) **Help to identify persons** who are unwilling to identify themselves or appear to be using someone else's identity or false identity where powers to take fingerprints are not available. It is in the public interest that the police are not hoodwinked by such subterfuge (resulting in wasted resources and increased risk) but provided with the tools to properly conduct their role and overcome such tactics.

(d) **Help identify a deceased person** or a person who is incapacitated or otherwise unable to identify themselves. It is important that the family are promptly informed and to do this, there is a need to promptly identify the deceased. RFR helps serve the public interest by speeding up the identification process and allowing the police to promptly contact family members and offer them early support when they might otherwise be seeking to find their deceased relative.

(e) **Protecting the custody environment** – it is important that both detainees and officers are safe in the custody environment. This is critical to the trust and confidence of those who are asked to police London and the wider public. RFR provides a way to enable the early identification and management of risk in the custody environment. It also enables the MPS to ensure it utilises the policing information it has at its disposal to ensure that a person in detention is considered against all information known to the police. This is in the public interest, particularly where bail decisions are made – RFR would allow the MPS to link the detainee to their involvement in other crimes (where they may have been previously unidentified) and in so doing, their risk profile be fully assessed. This helps keep the public safe.

(f) **Linking faces across different media**, even though no reference images are available. This will help with investigation of crimes happening repeatedly in the same location or in a number of locations but with the same method of operation. Such crimes have a particular blight on a local community, accordingly RFR meets a public interest in linking events together to develop a more complete intelligence picture that allows such crime to be more effectively tackled.

2.51 Any use of RFR needs to meet a 'Pressing Social Need'. In this regard the following Statutory Instrument passed in the context of the Data Protection Act 1998 is informative, in which it identified the prevention and detection of crime as an exemplar of a pressing social:

Statutory Instrument 2000/417:

1(1) The processing:

a) is in the substantial public interest;

b) is necessary for the purposes of the prevention or detection of any unlawful act;

c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

(2) In this paragraph, "act" includes a failure to act.

Are your actions / data-sharing a proportionate response to the social need this project / initiative has identified?

2.52 The MPS RFR Legal Mandate provides detailed analysis relating to Article 8 and wider human rights considerations in relation to the proportionate use of RFR.

2.53 Whilst not an exhaustive list, there are a number of safeguards and mitigations adopted by the MPS to enable the lawful and proportionate use of RFR. These safeguards are set out below.

(a) **Data Retention:** Controls have been implemented to minimise the unnecessary retention of personal data – particularly biometric data. The controls provide that:

(i) Where the RFR system does not generate a Potential Match, then a person's biometric data and Probe Image will be marked for deletion and automatically deleted from the RFR System unless the biometric template and facial image is retained as part of the Unresolved Crime Cache for ongoing searching in line with approval attached to that image. The biometric template and Probe Image will be deleted as soon as practicable following:

(ii) a Viable Match meaning the data no longer needs to be in the Unresolved Crime Cache;

(iii) the expiry of the relevant Tier period (as specified in the RFR Policy) – see paragraph 4.9(b) below; or

(iv) the investigation being otherwise resolved.

(b) Where the Probe Image is designated for inclusion with the Unresolved Crime Cache for a period of the image will be held in that cache for periods. Personnel will additionally be required to review Probe Images in RFR System every 3 months for Tier 3 offences (least serious), 6 months for Tier 2 and 9 months for Tier 1 (most serious) after submission to ensure the continuing need for the RFR Search. The Tiers are set out in Annex C of the MPS RFR Policy and have themselves been subject to a DPIA assessment as part of the FIMS facial library DPIA.

(c) Where the RFR system generates a Potential Match all personal data associated with a Probe Image is deleted as soon as practicable and in any case within 31 days except where:

(i) the Potential Match is confirmed as a Viable Match and then personal data is retained in accordance with the Data Protection Act 2018 and MOPI; and/or

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

(d) In relation to Image Reference Libraries, these are not dedicated resources linked to RFR and will be retained by the MPS in line with the policy applicable to them. From an RFR perspective, they will cease to be available for RFR Searching and deleted from any RFR system on expiry of any approval to use the Image Reference Library for RFR Searching.

(e) **Public Awareness:** Key MPS RFR Documents have been published with the MPS RFR Legal Mandate explaining how the use of RFR is both accessible and foreseeable particularly with reference to the MPS RFR Policy. This provides an answer such that the use of RFR by the MPS for its use-cases can be foreseen by the public. These points may be termed the 'What Question' and the 'How Question' and essentially go to the points where RFR results in inference with Article 8 Rights and involves sensitive data processing.

(i) The 'What Question' – this is a question as to what grounds enable a Probe Image to be used for RFR Searching? The MPS RFR Documents answer this by:

- placing controls and safeguards around the selection and use of Probe Images for RFR Searching including the adoption of a tiered approach to the selection of Probe Images that focuses consideration on the sources of Probe Images and the expectations of privacy that attach to such images;
- implementing specific controls and safeguards in relation to certain protected characteristics – including where a risk of exploitation may otherwise arise;
- outlining the criteria for when an RFR Search may be undertaken – this approach limits undue discretion and ensures that searches have a policing objective;
- specifying the process to undertake an RFR Search and the approvals that attach to RFR Searching; and
- detailing when images may be selected for ongoing RFR Searching against holdings against the MPS' Image Reference Libraries and the further controls and safeguards which attach to this process.

(ii) The 'How Question' – this is a question as to how Image Reference Libraries are to be searched and how officer decision making is channelled to ensure safeguards are in place to undertake a proportionate search, targeted on need as opposed to running a 'search all' or allowing undue levels of discretion. The MPS RFR Documents answer this by:

- outlining an approval process to approve an Image Reference Library as being eligible for RFR Searching both in relation to Substantive Image Reference Libraries with ongoing utility to the MPS and Temporary Image Reference Libraries of relevant to a specific investigation or operation;
- outlining the process by which approved Image Reference Libraries may be searched. The controls and safeguards are designed to recognise that different Image Reference Libraries have differing level of sensitivity

and it is necessary to ensure undue data processing is minimised when a less intrusive Image Reference Library would allow the policing objective to be achieved. Accordingly the MPS RFR Documents implement a staged process to RFR Searching; and

- providing direction to both those being asked to approve the use of an Image Reference Library for RFR Searching and those undertaking RFR Searching in terms of how Image Reference Libraries may be approached in terms of the intrusion and data processing that attaches to them and when elevated privacy considerations may arise.

(f) **Probe Images:** The MPS has adopted a number of controls and safeguards to ensure the currency, relevancy and suitability to submit a Probe Image for RFR Searching. These include:

(i) Selection: a human decision is needed to select Probe Images for RFR Searching – there is no automatic decision to submit for RFR Searching. This ensures the use of RFR is focused.

(ii) Managing collateral within a Probe Image:

(A) In respect of still images: the system operates an automatic face identification system that will only identify one facial image (the strongest for searching) from any number of faces that are present on the ingested image. In the case where there are, for example, 10 visible faces, only one will be selected for uploading as a probe. If the RFR operator is interested in one specific face amongst a number of faces, s/he will need to crop the image so that it only has the relevant face. This system protects collateral images and avoids inadvertent searching.

(B) In respect of video ingestion: the system operates an automatic face identification system that will identify each of the facial images that appear in the video and display them in a gallery. The RFR User will then select one or more facial images for searching against the relevant Image Reference Library.

(iii) Source / Expectations of Privacy: the need to consider the source of Probe Images including (i) the source of the image and any risk of compromise/risk to that source, (ii) where the image is non-compliant or otherwise obtained in circumstances where there are greater expectations of privacy. The use of the Probe Image 'Levels' system and the elevated privacy considerations position in the MPS RFR Policy Document embeds this approach.

(iv) Currency: controls around the currency of Probe Image with the most up to date and/or suitable image being used for RFR Searching unless there are particular reasons to search against a specific image.

(v) Suitability: 'by design' the RFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate responses.

(vi) Approval: the RFR Policy sets out the circumstances in which (A) a Probe Image may be used for RFR searching (which is dependent on, amongst other things the age and the nature of the offence);

(vii) Use: Probe Images may only be used for RFR Searching if they fall within specified categories which each link to an underlying policing purpose.

(viii) Ongoing searching: where the person requesting the RFR search considers it necessary the Probe image will be imported into the Unresolved Crime

Cache and searched for a period of 3, 6 or 9 months, as determined by the Tier of offence (specified in the RFR Policy), pending RFR User review/deletion. The continued use of the Probe image for the purpose of the prevention and detection of crime, while the crime remains unresolved, is considered to be proportionate, having regard to the pressing social need identified in this DPIA and will be authorised by an inspector (or equivalent).

(ix) Probe Images Collections: where it is deemed necessary to make a search of a collection of Probe Images, where those images have a common characteristic or are held for a common reason, the approval of an inspector (or equivalent) or above will be required in accordance with RFR Policy.

(g) **Image Reference Libraries:** The MPS has adopted a number of controls and safeguards to ensure the currency, relevancy and suitability of undertaking a RFR Search against an Image Reference Library is managed. These include:

(i) Methodology for use**:** the selection of the Image Reference Libraries for searching is specific to each RFR Search and informed by the intelligence case and policing need for that RFR Search; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching.

(ii) Temporary image Reference Libraries: the use of a limited-time, limited-purpose and access controlled Image Reference Library to limit the availability of images relevant to a specific investigation or operation from wider searching.

(iii) Human in the loop**:** the RFR system is designed to assist MPS personnel. The RFR system will always flag potential matches against an Image Reference Library to at least one officer for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.

(h) **Unresolved Crime Cache**: as noted above, Probe Images which are not matched with an image held in an Image Reference Library may (at the request of the officer initiating the RFR Search) be retained in the Unresolved Crime Cache for a period of the 3, 6 or 9 months (dependent on crime tier as explained in paragraph 2.28(b) above) pending RFR User review/deletion. Considerations relevant to including an image in the Unresolved Crime Cache are that:

(i) Matching within the Unresolved Crime Cache: Potential Matches of the Probe Image against other images within the Unresolved Crime Cache will be flagged to the RFR User for Adjudication. Searches against images within the Unresolved Crime Cache involve higher level of intrusiveness as compared to a search against the Custody Images Dataset, because of the higher level of intrusiveness associated with the inclusion of non-policing sources images (albeit those the public would expect the police to hold, in accordance with the levels set out in Annex A of the RFR Policy). Nevertheless, this searching will in many cases considered necessary on the basis of the immediate need to resolve the crime under investigation (and the officer submitting the image

(ii) Endorsement: it is acknowledged that inclusion in the Unresolved Crime Cache will entail a higher level of intrusion as compared with a simple RFR

Search. As a safeguard, a Probe Image will only be enrolled into this cache with the endorsement of a person of inspecting rank (or staff).

(iii) Currency: currency is ensured by the relatively short periods of retention in the unresolved crime cache (3, 6 or 9 months);

(iv) Human in the loop**:** as above, the matching will only occur after an adjudication by the RFR User who submitted the Probe Image for inclusion in the Unresolved Crime Cache.

The considerations relevant to Probe Images will also be relevant.

(i) **Approvals for RFR Searching:** the MPS has adopted a system where a level of approval is needed in order to return an RFR Search result – the level being proportionate to the expectations of privacy that are associated with the relevant imagery:

(i) Image Reference Libraries: to use any Image Reference Library for searching requires approval – from the MPS RFR SRO in the case of Substantive Image Reference Libraries and in the case of a Temporary Reference Library an officer (save in cases of urgency) of at least Superintending rank. This provides oversight and scrutiny from suitably senior personnel with experience of evaluating the policing need with the intrusions associated with a policing action.

(ii) Probe Images: RFR Users are able to undertake RFR Searches using Probe Images with the lowest levels of intrusion against Image Reference Libraries that have been approved for RFR Searching. To run a RFR Search using a more sensitive Probe Images the approval of at least Inspecting rank is required – such officers are familiar with privacy considerations and in other contexts, such as custody are already given legal powers under PACE for authorising the taking of other biometric data and undertaking searches using it.

(j) **Appropriate RFR Technology:** The MPS has carefully selected its RFR technology to provide high levels of statistical accuracy and demographic performance. The NPL has also undertaken specific operational testing of the MPS RFR system. The MPS has published a paper entitled 'The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its RFR algorithm, including undertaking a process of peer review. The high levels for performance identified by the document have fed into the MPS RFR Documents including safeguards in the MPS RFR Policy. As technology continues to improve, the MPS will continue to review its RFR capability to ensure that performance is maximised, that intrusion is minimised, and to ensure that RFR Searching remains proportionate to the policing purposes. When a new algorithm is considered for use, the MPS will need to make a determination, as to whether it is fit for its law enforcement purposes, whilst reviewing the proposed safeguards to ensure that they remain sufficient and relevant.

(k) **Technical and Security** Measures: the RFR System has the following security features:

(i) All data processed by the RFR System is internally secured through data encryption.
(ii) All data at rest is encrypted including biometric templates
(iii) Standard Foundation accounts will be used to manage each MPS user's identity for The RFR System. MPS Single Sign-On will be enabled.
(iv) Access is restricted to authenticated and authorised RFR Users.
(v) Timeouts will be configured as required. It is recommended that user sessions timeout after a set period of inactivity and after a set number of hours regardless of activity.
(vi) The RFR System application has native antivirus scanning functionality and all files uploaded will be scanned
(vii) NEC has a security incident and response process encompassed by the Cyber Security Breach Response Plan.

(l) **Review:**

(i) Adjudication - RFR Search results: All RFR Searches are subject to human-in-the-loop decision making – a Potential Match only becomes a Validated Match following a human review via the Adjudication process. In order to minimise confirmation bias issues training is provided to RFR Users to identify and address this risk.
(ii) Ongoing: RFR Searching and the materials that support RFR Searches will be subject to periodic review to ensure that the RFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

(m) **Consideration of Alternative Policing Tools:** The use of RFR by the MPS will be considered alongside other policing tools and tactics. Consideration will be given as to the effectiveness and intrusiveness of other viable methods that might produce the same result, with the least intrusive, viable method being adopted to progress an investigation.

(n) **Training:** training to be provided to all RFR users prior to their authorisation to undertake searching on the RFR System.

2.54 At the outset, the RFR System will search Probe Images against the Custody Images Dataset and against the Unresolved Crime Cache. Specific measures to ensure the proportionality of the use of the Custody Images Dataset are set out in paragraphs 2.28 – 2.31, above.

2.55 The proportionality of the inclusion of the 13-15 MOPI Group 3 CONNECT Cohort is considered in 2.37 – 2.39.

Common Law Duty of Confidence

A breach of confidence will become actionable if:-

1. the information has the necessary quality of confidence; *and*
2. the information was given in circumstances under an obligation of confidence; *and*
3. there was an unauthorised use of the information to the detriment of the confider (the element of detriment is not always necessary).

However, there are certain situations when a breach of confidence is not actionable. Those situations are:-

1. a person has provided consent for the processing of their information; *and*
2. there is a legal requirement to process the information; *and*
3. it is in the public interest to process the information.

4.12 It is the view of the MPS that (i) there is a legal requirement to process the information, and (ii) it is in the public interest to process the information. This is further detailed in the MPS RFR Legal Mandate.

4.13 Beyond personal data (as defined by the DPA 2018), the MPS RFR Legal Mandate also recognises that a duty of confidence may arise in relation to the processing of imagery that relates to the deceased.

Data Protection Act 2018 - Principle 1

1. The processing of personal data for any of the law enforcement purposes must be lawful and fair;

2. The processing of personal data for any of the law enforcement purpose is lawful only if and to the extent that it is based on law and either:-

    a. the data subject has given consent to the processing for that purpose; *or*
    b. the processing is strictly necessary for the law enforcement purpose. It must be stressed that the MPS has no intention to provide wide access to this data (whether within or outside of the MPS). Nor indeed is it our intention to process this data beyond our core policing purposes; *and*
    c. the processing meets at least one of the conditions in Schedule 8.

4.14 The MPS RFR Legal Mandate outlines:

(a) the legal basis on which RFR may be used by the MPS and the legal basis for the RFR Searching of the Custody Images Dataset;

(b) the grounds required where RFR may be used on the basis that it is strictly necessary for a law enforcement purpose;

(c) confirmation that a condition of Schedule 8 will be met;

(d) how the MPS upholds the Public Sector Equality Duty.

4.15 The MPS RFR Legal Mandate and the other MPS RFR Documents also explains how the MPS processes data fairly. Fairness is particularly relevant in three respects:

(a) Accessibility: The RFR Legal Framework which underpins the MPS's RFR capability benefits from a number of steps to ensure it is sufficiently accessible to meet the quality of law test. In particular the RFR Legal Framework benefits from primary legislation for its use of custody images and a number of other case-specific use-cases identified in this legal mandate, published and often-cited case law and a Code of Practice (in relation to PACE).

(b) In relation, particularly to use-cases for RFR Searching where the legal basis is the common law, the Court of Appeal in *Bridges* recognised that published policy documents can also enable a police force to comply with the quality of law requirement. Recognising that in this particular instance, certain matters such as when an RFR Search may be undertaken require policy in order to meet the quality of law test, specifically around foreseeability, the MPS has published its RFR Policy Document.

(c) Foreseeability: The use of RFR, particularly when under common law, should be undertaken in a way that is predictable. It does not require "an over-rigid regime which does not contain the flexibility which is needed to avoid unjustified interference with a fundamental risk" but does mean "safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate interference with Convention rights".

(d) In Bridges, in the context of live facial recognition, the court recognised two questions arose that conferred too greater a discretion on officers to determine policy on a case-by-case basis such that the overall use of live facial recognition in that specific case was found not to be foreseeable and therefore in accordance with law. These two questions where termed by the Court of Appeal to be the 'Who Question' and the 'Where Question' – in essence who could be placed on a LFR Watchlist for location and where LFR could be deployed to locate the people on an LFR Watchlist. A similar position exists for RFR and the questions for the MPS are addressed by way of a published policy. This provides an answer such that the use of RFR by the MPS for its use-cases can be foreseen by the public. These points may be termed the 'What Question' and the 'How Question' and essentially go to the points where RFR results in inference with Article 8 Rights and involves sensitive data processing.

(e) Fairness 'by design': The MPS has published a paper entitled 'Understanding the Metropolitan Police Service RFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its RFR algorithm. In this regard it is reassuring that the NPL study of the RFR System did, in fact, find it to be 100% statistically accurate in the testing

they undertook, as reported in the "Facial Recognition Technology in Law Enforcement Equitability Study" (2023).

4.16 Additionally, in relation to fairness, the MPS has also taken the following measures:

(a) Ongoing reviews to mitigate risks of unfairness: Informed by its Equality Impact Assessment, the MPS RFR Documents already provide for ongoing evaluation of the RFR system. This also offers the MPS a chance to monitor for technical issues and trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS's Facial Recognition Strategic Board which reviews the performance of the RFR system at a strategic level.

(b) Control measures to ensure fairness: the MPS will use the statistical reports produced by the RFR System that report on demographic issues relating to matching identify anomalous RFR User performance. RFR Users will have training to ensure the RFR System is used compliantly and that retention protocols are followed.

4.17 The MPS has specifically considered the U16 MOPI 3 CONNECT Cohort Issue in the context of fairness, in particular the question of whether it is fair that the children with images who have been captured in the age range of 13-15 held on the CSIS/CIS systems would not form part of the Custody Image Dataset, but those held in the CONNECT custody image database will. The MPS have concluded overall that the disparity of treatment is fair overall, when the objective of the processing is considered. The alternatives that would ensure fairness are the exclusion of aged 13-15 Cohort from the RFR System (CONNECT, CSIS & CIS) or for the relatively small (but growing) number of MOPI Group 3 cohort to be included, with the major detriment to the policing objective that this would entail or for the unfairness to persist until the schedule "fix" occurs. As noted above, the MPS considers that the decision to include the MOPI Group 3 CONNECT cohort is proportionate.

Describe whether you rely on consent to process personal data, and how this consent will be obtained? If obtaining consent (see explanation below) would prejudice the purpose of the data collection, what legal basis do you rely on?

Note: Consent from data subjects, is not always relied upon as a legal basis to process data. This is because consent can be withdrawn by the data subject at any time. If consent is withdrawn, the MPS must either delete the data or demonstrate another legal basis for processing the data.

Consent will not be sought. The MPS will process personal data on the basis that it is strictly necessary for a law enforcement purpose.

Data Protection Act 2018 - Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.18 Personal information must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes.

4.19 RFR only uses information held by policing which has therefore already been assessed for relevance to a law enforcement purpose in order to justify its retention. In relation to the personal data collected and processed by the RFR system, the following additional measures apply:

(a) **Legitimate aim drives processing:** As the use of RFR is an operational one, the person seeking to undertake the RFR search is required to identify a legitimate aim and legal basis for that search. Key considerations relating to necessity and proportionality are addressed by the RFR process. The processing is also undertaken under Part III of the DPA 2018 which requires a law enforcement purpose to apply (as defined by Section 31 of that Act).

(b) **Explicit purposes and purpose limitations** The use of RFR 'Levels' driving when approval is required – this being particularly relevant for more sensitive Probe Images (which require at least Inspecting rank approval) and for all Image Reference Libraries. The approval process for Image Reference Libraries requires the SRO to approve the types of Probe Image that may be used for searching (for example, the SRO may approve a ' use case for those suspected of offences but exclude searching against missing persons). Should a further law enforcement purpose be identified outside of the scope of the RFR Form 1 use case, consideration would need to be given for an amendment to that form, with the further approval of the Authorising Officer.

(c) **Management of collateral:** The RFR System is designed to minimise collateral intrusion and unnecessary data processing that would fall outside of the 'explicit' processing criteria.

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

(e) Audit log data is stored in a read-only database, ensuring that once written, data cannot be modified. Access to review audit data is provided as part of a separate web-based administrative client and only granted to authorised users through the integrated Role Based Access Control (RBAC).

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

(g) **Oversight by the FR Board**: Within the MPS, the senior internal oversight body for RFR is the MPS FR Technology Board, which in-turn answers to the MPS Management Board. In addition, MOPAC provide oversight and scrutiny while the London Policing Ethics Panel provide independent insight and guidance.

(h) The MPS FR Technology Board is empowered by this policy to assist the SRO in relation to the use of Image Reference Libraries, but is also responsible for assuring the suitability of the MPS RFR Policy Documents and assisting the SRO to maintain oversight as to lawful, ethical and effective use of RFR.

Have you identified potential new purposes as the scope of the project expands? If the answer to this question is 'yes', then you must seek the advice of the ISSU.

No.

Data Protection Act 2018 - Principle 3

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

4.20 The MPS RFR Documents provide that the MPS will only process data that is relevant and proportionate to its law enforcement policing purposes. There are a number of systems and processes in place to ensure this. These are set out below:

(a) **Approvals for RFR Searching:** the MPS has adopted a system where a level of approval is needed in order to return an RFR Search result – the level being proportionate to the expectations of privacy that are associated with the relevant imagery:

(iii) Image Reference Libraries: to use any Image Reference Library for searching requires approval – from the MPS RFR SRO in the case of Substantive Image Reference Libraries and in the case of Temporary Image Reference Libraries, an officer (save in cases of urgency) of at least Superintending rank. This provides oversight and scrutiny from suitably senior personnel with experience of evaluating the policing need with the intrusions associated with a policing action. As part of this process, the approval for the Image Reference Library may limit the types of Probe Images that may be searched against it. This is to ensure that relevant searches are undertaken.

(iv) Probe Images: RFR Users are able to undertake RFR Searches using Probe Images with the lowest levels of intrusion against Image Reference Libraries that have been approved for RFR Searching. To run an RFR Search using a more sensitive Probe Images the approval of at least

Inspecting rank is required – such officers are familiar with privacy considerations and in other contexts, such as custody are already given legal powers under PACE for authorising the taking of other biometric data and undertaking searches using it. This provides assurance as to the necessity for the data processing to be undertaken.

(b) **Probe Images:** The MPS has adopted a number of controls and safeguards to ensure the currency, relevancy and suitability to submit a Probe Image for RFR Searching to ensure that unnecessary data processing is minimised. These include:

(i) Selection: a human decision is needed to select Probe Images for RFR Searching – there is no automatic decision to submit for RFR Searching. This ensures the use of RFR is focused.

(ii) Managing collateral within a Probe Image: The RFR System is designed to minimise collateral intrusion and unnecessary data processing that would fall outside of the 'explicit' processing criteria.

(iii) Currency: controls around the currency of Probe Image with the most up to date and/or suitable image being used for RFR Searching unless there are particular reasons to search against a specific image. This ensures the most relevant images are used as Probe Images for RFR Searching.

(iv) Suitability: 'by design' the RFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate responses. This ensures that searches are undertaken when it is suitable to do so and it is assessed that the results could provide information of relevance to the legitimate aim.

(v) Approval: the RFR Policy sets out the circumstances in which (A) a Probe Images may be used for RFR searching (which is dependent on, amongst other things the age and the nature of the offence);

(vi) Use: Probe Images may only be used for RFR Searching if they fall within specified categories which each link to an underlying policing purpose. This ensures a relevance to a law enforcement purpose.

(c) **Appropriate RFR Technology:** The MPS has carefully selected its RFR technology to provide high levels of statistical accuracy and demographic performance. The NPL has also undertaken specific operational testing of the MPS RFR system. The MPS has published a paper entitled 'The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its RFR algorithm, including undertaking a process of peer review. The high levels for performance identified by the document have fed into the MPS RFR Documents including safeguards in the MPS RFR Policy. As technology continues to improve, the MPS will continue to review its RFR capability to ensure that performance is maximised, that intrusion is minimised, and to ensure that RFR Searching remains proportionate to the policing purposes. When a new algorithm is considered for use, the MPS will need to make a determination, as to whether it is fit for its law enforcement purposes, whilst reviewing the proposed safeguards to ensure that they remain sufficient and relevant.

(d) **Review:**

(i) Adjudication - RFR Search results: All RFR Searches are subject to human-in-the-loop decision making – a Potential Match only becomes a Validated Match following a human review via the Adjudication process. This process is to ensure the accuracy and relevancy of results, to link them with other policing information and therefore minimise unnecessary data processing and intrusion until MPS are satisfied with the accuracy of the results.

(ii) Ongoing: RFR Searching and the materials that support RFR Searches will be subject to annual review by the FR Board to ensure that the RFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case. Processing mechanisms, RFR policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes.

(e) **Data Retention:** Controls have been implemented to minimise the unnecessary retention of personal data – particularly biometric data. The controls provide that:

(i) Where the RFR system does not generate a Potential Match, then a person's biometric data and Probe Image is marked for deletion and then automatically deleted from the RFR System unless the biometric template and facial image is retained as part of the Unresolved Crime Cache for ongoing searching in line with approval attached to that image. Then the biometric template and Probe Image deleted as soon as practicable following the earlier of:

(A) a Viable Match meaning the data no longer needs to be in the Unresolved Crime Cache;

(B) the resolution of the investigation by means other than the RFR System; and

(C) following the expiry of the approval for the use of the Unresolved Crime Cache specified in the Tier.

(ii) Where the RFR system generates a Potential Match all personal data associated with a Probe Image will be deleted as soon as practicable and in any case within 31 days except where:

(A) the Potential Match is confirmed as a Viable Match and then personal data is retained in accordance with the DPA 2018 and MOPI; and/or

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

(iii) In relation to Image Reference Libraries, these are not dedicated resources linked to RFR and will be retained by the MPS in line with the policy applicable to them. From an RFR perspective, they will cease to be available for RFR Searching and deleted from any RFR system on expiry of any approval to use the Image Reference Library for RFR Searching.

4.21 **Specific issues relating to the use of the Custody Image Dataset**:

(a) **Outstanding reviews of custody images:** The MPS has adopted safeguards to ensure that images are within the time period for retention permitted by MOPI (dependent on crime type) without reference to any extension to that initial period that may be permitted by a manual review of the relevant personal data.

(b) **Unconvicted data subjects (where the case is NFA (not charged, de-arrested) or no conviction):** the MPS complies with the Home Office guidance document "Review of the Use and Retention of Custody Images" (2017).

(c) **Juvenile detainees**: the MPS has adopted the safeguards set out in paragraph 2.31 above to ensure the proportionality of the RFR System searching.

(d) **U16 MOPI 3 CONNECT Cohort Issue**: this issue is considered at paragraphs 2.37 to 2.39 above. Although the MPS acknowledges the processing of the 13-15 MOPI 3 CONNECT Cohort is sub-optimal (and will be resolved as a matter of priority), it remains necessary and proportionate to include the set on a temporary basis, pending the technical fix.

Which personal data could you not use, without compromising the needs of the project?

4.22	All personal data processing will be strictly necessary and proportionate to the legitimate aim of the relevant RFR Search. The MPS has carefully evaluated the personal data to be used during RFR Searching and as part of that process has positively identified areas where it does not need to process personal data and excluded those from the design of the RFR system. For example, the RFR System is designed to minimise collateral intrusion and unnecessary data processing that would fall outside of the 'explicit' processing criteria.

Data Protection Act 2018 - Principle 4

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

4.23 The MPS is mindful of the potential damage and distress to data subjects, organisations, and to third parties if inaccurate data is processed in any way. To mitigate this, the RFR system used by the MPS has been carefully considered by the MPS to ensure its statistical accuracy. Additionally, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing. There are a number of measures and controls in place to ensure statistical accuracy and the accuracy of personal data. These are set out below.

(a) **Statistical accuracy:** The ICO has provided helpful guidance on their expectations for statistical accuracy. They note that the accuracy principle "does not mean that the RFR system needs to be 100% statistically accurate to comply with the accuracy principle." The ICO does however recognise the importance of considering the accuracy of the RFR system at the outset, including evaluating claims made by the vendor. In this respect the MPS has paid close regard to the NIST findings. In this regard it is also therefore reassuring that the NPL study of the RFR System did, in fact, find it to be 100% statistically accurate in the testing they undertook, as reported in the "Facial Recognition Technology in Law Enforcement Equitability Study" (2023).

(b) **Probe Image Currency:** The MPS has adopted a number of controls and safeguards to ensure the currency, relevancy and suitability to submit a Probe Image for RFR Searching to ensure that unnecessary data processing is minimised. In relation to Principle 3, these include controls in the MPS RFR Policy around the currency of Probe Image with the most up to date and/or suitable image being used for RFR Searching unless there are particular reasons to search against a specific image.

(c) Technical measures are in place to ensure pre-RFR Checks have been conducted including confirming the person remains of relevance to the MPS's investigations prior to undertaking an RFR Search. This protection is part of the MPS's commitment to taking all reasonable steps possible in ensuring that personal data that is inaccurate, incomplete, or no longer up-to-date, is not made available or used for RFR Searching

(d) **Probe Image Quality:** 'by design' the RFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate responses.

(e) **Management of Collateral / Distinguishing Data Subjects:** The RFR System is designed to minimise collateral intrusion and unnecessary data processing that would fall outside of the 'explicit' processing criteria.

(f) **Adjudication:** All RFR Searches are subject to human-in-the-loop decision making – a Potential Match only becomes a Validated Match following a human review via the Adjudication process. In order to minimise confirmation bias issues training is provided to RFR Users to identify and address this risk.

(g) **MPS Policy:** The MPS upholds the rights of individuals under the DPA 2018. The MPS has policies and procedures that help to ensure that inaccurate information can be updated. This includes the MPS Privacy Notice, which provides measures that allow the public to correct inaccurate information that may be held about them.

If the MPS is procuring new software, does it allow the data to be amended / deleted when necessary? The answer to this question must always be yes. The system should also enable the

ability to note that the accuracy of information has been challenged and why.e accuracy of information has been challenged and why.
4.24 Yes. Measures are in place regarding other personal data as outlined elsewhere in this DPIA.
How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?
4.25 MPS personnel will take all reasonable steps to ensure that the Probe Image and the data associated with it is accurate. When adding an image to the RFR system, the RFR system will assess it for quality and suitability for matching, in order to allow MPS personnel to consider and manage the risk that poor quality images generate inaccurate RFR matches.
Data Protection Act 2018 - Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose for which it is processed.
The information will be retained in line with our Retention, Review and Deletion Policy and the MPS RFR Documents. These are subject to at least annual review.
What retention periods are suitable for the personal data the MPS will be processing?

4.26 Controls have been implemented to minimise the unnecessary retention of personal data – particularly biometric data. The controls provide that:

(a) Where the RFR system does not generate a Potential Match, then a person's biometric data and Probe Image will be scheduled for deletion from the RFR System unless the biometric template and facial image is retained as part of the Unresolved Crime Cache for ongoing searching in line with approval attached to that image. The biometric template and Probe Image will be deleted as soon as practicable following:

(i) a Viable Match meaning the data no longer needs to be in the Unresolved Crime Cache;

(ii) the expiry of the relevant Tier period (as specified in the RFR Policy); or

(iii) the investigation being otherwise resolved.

(b) Where the RFR system generates a Potential Match all personal data associated with a Probe Image is deleted as soon as practicable and in any case within 31 days except where:

(i) the Potential Match is confirmed as a Viable Match and then personal data is retained in accordance with the Data Protection Act 2018 and MOPI; and/or

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

(c) In relation to Image Reference Libraries, these are not dedicated resources linked to RFR and will be retained by the MPS in line with the policy applicable to them. From an RFR perspective, they will cease to be available for RFR Searching and deleted from any RFR system on expiry of any approval to use the Image Reference Library for RFR Searching.

(d) For the MVP version of the RFR System it is anticipated that the only Image Reference Library will be searchable will be the Custody Images Dataset. The retention period applicable to the Custody Image Dataset are set out in paragraphs 2.28 – 2.31, above. As noted above, the Custody Image Dataset will be linked by a 'delta-link' to the custody images holdings, and this will provide that any images that is deleted from the underlying data holdings will also be deleted from the Custody Image Dataset. The Unresolved Crime Cache will also be operational and will operate with the review period specified in paragraphs 2.28(b), above.

Are you procuring software that will allow the MPS to delete information in line with the corporate retention policy?

Yes.

Data Protection Act 2018 - Principle 6

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

Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
4.27 The RFR system includes a number of physical and technical security measures. These include: a. All data processed by the RFR System is internally secured through data encryption. b. All data at rest is encrypted including biometric templates c. Standard Foundation accounts will be used to manage each MPS user's identity for The RFR System. MPS Single Sign-On will be enabled. d. Access is restricted to authenticated and authorised RFR Users. e. Timeouts will be configured as required. It is recommended that user sessions timeout after a set period of inactivity and after a set number of hours regardless of activity. f. The RFR System application has native antivirus scanning functionality and all files uploaded will be scanned g. NEC has a security incident and response process encompassed by the Cyber Security Breach Response Plan. 4.28 **Further Measures**: include the following features: h. The solution is hosted in the MPS' Azure secure environment; i. Users have to logon to MPS which is then passed onto RFR via SSO; j. Role based access conditions will limit the functionality available and access to data, enforcing the principles of least privilege and need-to-know k. Azure leveraged security products including Prometheus and Grafana, Azure Security Centre, and Qualys. l. All traffic will traverse existing Azure Expressway connections, it will not pass over the internet and is encrypted at rest and in transit (HTTPS). m. Logging, alerting and auditing will be in place and supported by the relevant MPS tower. n. An SDLC process will be in place to ensure artefacts received by suppliers are free from security vulnerabilities 4.29 The MPS RFR Documents outlines the actions that must be taken in the event that personal data is lost. The RFR systems security measures serve to minimise the data risks and impact arising from such a loss. 4.30 The MPS undertakes vetting checks on its personnel appropriate to their role. 4.31 The MPS RFR Documents and other relevant documents such as those relating to information security are subject of regular review. 4.32 **Security Against Unlawful Processing**: The MPS RFR Documents set out the structures that enable and support lawful RFR Searching and the approvals that attach to the use of Probe Images and Image Reference Libraries.

Safeguards – Archiving
Personal and special category data shall be processed where the processing is necessary for archiving purposes in the public interest.
4.33 Refer to section 5. Balanced Risk Assessment below. Schedule 8 conditions will apply to RFR processing on the grounds that the processing is strictly necessary for a law enforcement purpose.
Safeguards – Sensitive Processing
The processing of personal and special category data is reliant on the consent of the data subject and reliant on a DSA, or reliant on a condition specified in schedule 8.
4.34 Refer to section 5. Balanced Risk Assessment below. Schedule 8 conditions will apply to RFR processing on the grounds that the processing is strictly necessary for a law enforcement purpose.
Complaint Handling
Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection Officer.

4.35	Complaints about the use of Personal Information in relation to this project should be handled by the MPS DPO.
Freedom of Information Act 2000 (FoIA)	
4.36	In meeting its FoIA obligations, the MPS is committed to maintaining an open and transparent approach regarding the processing outlined within this DPIA. This is subject to any exemptions that may apply under FoIA, including those relating to security or confidentiality.
4.37	The MPS is a public authority for the purposes of the FoIA. This means that information held by the MPS is accessible to the public on written request, subject to limited exemptions.
4.38	In accordance with guidance from the ICO, the MPS will place this DPIA and other associated MPS RFR Documents onto our FoIA Publication Scheme, helping to raise public awareness of how the MPS processes personal data. Any exception to this will meet FoIA criteria.
4.39	All public requests for information should be directed to the MPS DPO.
Individual Rights	
4.40	Part 3, Chapter 3 of the DPA 2018 applies to competent authorities processing data for law enforcement purposes. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
Transfers Outside the European Union (EU)	
4.41	Part 3, Chapter 5 of the Data Protection Act 2018 applies to the transfer of any personal data to a relevant authority/relevant international organisation in any third country.

Individual Rights

Data Protection Act 2018 – right to be informed

4.42 The MPS has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of the MPS to be open and transparent (wherever appropriate and possible) about how data is processed. To this end, and having considered the risks to this right posed by the use of RFR, the MPS has adopted a number of measures to ensure that the right to be informed is upheld.

4.43 A key measure is the publication of the MPS Privacy Notice, the MPS policy on protecting special category and criminal convictions, and key MPS RFR Documents on the MPS website. Whilst the MPS is not required to publish a number of these documents, it has elected to do so to help Londoners understand the standards the MPS, as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to use RFR, details about how RFR may be used, and the considerations and constraints relevant as to searching using Probe Images and Image Reference Libraries. In this way, the MPS's use of RFR is both foreseeable and assessable. The published documents provide information as set out in the table below.

Key documents available to the public	Information included
MPS Privacy Notice:	• Data Controller identity and contact details • Data Protection Officer details • The scope and purposes for processing personal data by the MPS • Data retention periods • Data sharing arrangements • Data security • Rights as a data subject (including access, rectification and erasure) • Complaints (including the right to make a complaint to the ICO and contact details).
MPS policy on protecting special category and criminal convictions	• The MPS approach in relation to protecting and processing special category and criminal convictions data in relation to the data protection principles • The responsibilities of the Data Controller • Information relating to erasure and retention • How further information may be sought.
MPS RFR Legal Mandate	• The lawful basis for processing data in relation to RFR. Including in relation to: o Police and Criminal Evidence Act 1984 o Specific legal powers identified on a case-by-case basis o Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Data Protection Act 2018 o Freedom of Information Act 2000
MPS Policy Document	• The RFR Policy.
MPS RFR DPIA	• Describes the nature, scope, context and purposes of the processing. • Assesses necessity, proportionality and compliance measures. • Identifies and assesses risk to individuals. • Identifies any additional measures to mitigate those risks.

MPS RFR Appropriate Policy Document	• Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the DPA 2018. • Explains how the MPS complies with the Law Enforcement data protection principles. Outlines policies as regards the retention and erasures of personal data.
Understanding The Metropolitan Police Service RFR System's Accuracy and Bias Position	• Explains in a public-facing summary: o how to understand RFR system accuracy; o what the MPS have done to understand its algorithm within an operational context, including commissioning the NPL Study.

Are you content that the MPS privacy notices covers the intended processing?

4.44 I have read the MPS Privacy Notice, and when read in conjunction with MPS RFR Documents, I am content that they sufficiently address the intended processing.

Data Protection Act 2018 – right of access

4.45 The right of access allows individuals to access their personal data and supplementary information, subject to certain restrictions. This right allows individuals to be aware of and verify the lawfulness of the processing the MPS is carrying out. The use of RFR does not fetter the right of access and processes are in place to facilitate requests received by the MPS including:

- **MPS Privacy Notice:** This notifies data subjects of their right to access, enabling them to receive a copy of the personal information held by the MPS and to check that the MPS are lawfully processing it and that it is accurate.

- **Dedicated MPS webpage:** A specific webpage outlines an individual's right of access. It provides details to data subjects about when the police will disclose information held about them and the process by which a request can be made. Where information can be provided, it is provided without charge.

- **Governance:** MPS policy and guidance is provided by the MPS's Information Rights Unit to ensure the MPS complies with this legal obligation.

Data Protection Act 2018 – the right to rectification

4.46 The right to rectification enables data subjects to have any incomplete or inaccurate information the MPS holds about them corrected. Data subjects are able request the rectification of police data that may be used for RFR Searching. The RFR process draws on existing MPS data for RFR Searching allowing existing MPS processes to be used to enable data subjects to exercise their right of rectification.

4.47 Additionally to uphold the right to rectification, the MPS has taken a number of further measures including:

- **MPS Privacy Notice**: This provides that requests for data rectification may be provided to the Information Rights Unit at: SARenquiries@met.police.uk or via post to PS Information Rights Unit, PO Box 313, Sidcup, DA15 0HH.

- **MPS website:** This provides the public with a copy of the MPS Privacy Notice that details h ow the right to rectification may be exercised.

- **Governance:** MPS policy and guidance is provided by the MPS's Information Rights Unit to ensure the MPS complies with this legal obligation.

Data Protection Act 2018 – the right to erasure and restriction

4.48 The right to erasure allows data subject to request erasure of their personal information. This enables data subjects to ask the MPS to delete or remove personal information where there is no lawful reason for the MPS to continue to process it. This right is not specific to RFR but applicable to all personal data processed by the MPS. RFR therefore does not restrict this right – in fact, the data created by RFR which no longer need to be retained is to be deleted in accordance with the established process. This includes:

1. Probe Images will be deleted where there is no basis for retention (or submission to Unresolved Crime Cache);

2. Images held within the Unresolved Crime Cache will be reviewed in accordance with period specified by their relevant Tier (as set out in the RFR Policy document).

3. Images held within the Image Reference Library will be subject to MOPI retention period, but also subject to annual review.

4. Images held in the Custody Image Dataset will be deleted on the earlier of: (i) their deletion from the MPS custody image database (with the deletion occurring by means of the 'delta link' between the custody image database and the Custody Image Dataset or (ii) the expiry of the periods set out in paragraph 2.12.

4.49 Right to restriction enables the data subject to ask the MPS to suspend the processing of personal information about the data subject, for example if they want the MPS to establish its accuracy or the reason for processing it. This right is not specific to RFR but applicable to all personal data processed by the MPS with established processes in place to facilitate such requests.

4.50 Additionally to uphold the right to erasure and restriction, the MPS has taken a number of further measures including:

- **MPS Privacy Notice**: This provides that requests for data erasure or restriction may be provided to the Information Rights Unit at: SARenquiries@met.police.uk or via post to PS Information Rights Unit, PO Box 313, Sidcup, DA15 0HH.

- **MPS website:** This provides the public with a copy of the MPS Privacy Notice that details how the right to erasure or restriction may be exercised.

- **MPS policy:** and guidance is provided by the MPS's Information Rights Unit to ensure the MPS complies with this legal obligation.

Occasions when individual rights may be limited

4.51 In accordance with Section 48 of the DPA 2018, the MPS may limit the provision of information where it is necessary and proportionate to:

1. avoid obstructing an official or legal inquiry, investigation or procedure;
2. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
3. protect public security;
4. protect national security; and
5. protect the rights and freedoms of others.

4.52 This is not a point that is specific to RFR but a consideration for requests relating to police information more generally. Where a limit is imposed, the MPS will inform the data subject of such limit, explaining the reasons for it and their right of redress via the ICO and the courts. The MPS will always record decision and the reasons for it but may not be obliged to notify the individual where notification itself would undermine the purpose of the limit.

Data Protection Act 2018 – the right not to be subject to automated decision-making

4.53 Part 3 of the DPA 2018 provides safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. without human intervention. Individuals have the right not to be subject to a decision when:

1. İt is based on automated processing; and
2. it produces an adverse legal effect or a significantly affects the individual.

4.54 In the context of upholding this individual right, the mandatory Adjudication process based around the need for a human-in-the-loop to make decisions is a crucial safeguard adopted by the MPS for its RFR Searches.

4.55 All RFR Searches are subject to human-in-the-loop decision making – a Potential Match only becomes a Validated Match following a human review via the Adjudication process. In order to minimise confirmation bias issues training is provided to RFR Users to identify and address this risk.

Consultation Results

Stakeholder Engagement and Consultation

The MPS has undertaken an engagement and consultation process. As a result, the stakeholders set out below were identified as being relevant to the data processing involved with the MPS's use of RFR. This has helped to shape the ongoing engagement and consultation process.

The engagement and consultation process has helped inform the MPS's understanding of how RFR and data processing engages human rights, including privacy, and how these should be dealt with. A transparent approach has been, and continues to be, important to building trust and confidence in the legitimacy of approach taken by the MPS.

Engagement and consultation will continue, as will the process of identifying relevant stakeholders. The DPIA continues to be a living document subject of the idiosyncrasies and vagaries of differing requirements for RFR, and as the MPS continues to review and learn from its use of RFR.

Stakeholders	**Roles and Responsibilities**	**Outcomes**
Must only be conducted through the Information Law and Security Group.	*Provision of guidance on completion of the DPIA and Pilot Exercise.*	*Advice issued.*

Public Consultation

No specific public consultation has been carried out or is planned, but surveys relating to the use of technology for policing purposes, such as the one set out in paragraph 2.21 are undertaken on a continuous basis.

Stakeholder Engagement and Consultation

The MPS has undertaken an engagement and consultation process. As a result, the stakeholders set out below were identified as being relevant to the data processing involved with the MPS's use of RFR. This has helped to shape the ongoing engagement and consultation process.

The engagement and consultation process has helped inform the MPS's understanding of how RFR and data processing engages human rights, including privacy, and how these should be dealt with. A transparent approach has been, and continues to be, important to building trust and confidence in the legitimacy of approach taken by the MPS.

Engagement and consultation will continue, as will the process of identifying relevant stakeholders. The DPIA continues to be a living document subject of the idiosyncrasies and vagaries of differing requirements for RFR, and as the MPS continues to review and learn from its use of RFR.

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.	2016 - 2020 on going consultations.	On 5th Jan 2021 the DMPC gave MOPAC approval for the MPS to go to the commercial market to identify a suitable product, vendor and a compliant route to market.

	Early Engagement over the concept of implementation. To seek views to support procedural best practice Seek IAM approval to go to the commercial market to identify possible vendors and products to fit the MPS business need.	Dec 2020 / Jan 2021	MOPAC are represented at the MPS FRT Strategic Board.
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. 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 -	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.
MPS Independent Advisory Groups (IAG) – Race IAG, LGBTQ+ IAG & Disability IAG.	MPS AIG attendees consist of members of the public representing the protected characteristics of race, disability, sexual orientation and gender. Consulted to attain public view points and assist with the identification of equality impact.	Ongoing consultation	Members were given an update on the MPS current position in respect to RFR. 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: ▪ The retention of images/data ▪ The existence of ethnic bias ▪ Transparency ▪ Public Trust ▪ Necessity

	Central Race IAG	21st August 2023	The IAG representatives offered feedback on potential different community perspectives of RFR and were pleased with the safeguards. Updates given to the group in relation to proposed use, functionality, policy and safeguarding. Members were given a point of contact to liaise with should they have any further points to raise or if further clarification is needed. 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. Group broadly supportive of the technology. Group to be given a demonstration in October 2023 at NSY of the technologies available.
South Wales Police FRT Team	SWP have implemented facial recognition technology trials (LFR and a fully operational RFR system. MPS have conducted a bench marking exercise to discuss their	Ongoing consultations between 2019-to date	Engagement continues with SWP at a both a national (NPCC) and force level to ensure best practice.

	governance and SOPs, to evaluate best operational 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. 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. 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. 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. 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.
Violent Crime Taskforce	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 RFR 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. 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	Ongoing	Ongoing consultation and engagement

	detection alert results across diverse facial variants. To seek confirmation of the ability to effectively capture and monitor diversity data to determine the existence of future bias across facial detection accuracy		
MPS Crime Prevention, Inclusion & Engagement Team (CPIE)	Consult on the implementation of RFR on their impacted business area	Ongoing	Ongoing consultation and engagement inc with a wider variety of CPIE stakeholders.
MPS Staff Support associations Association	To gain insight on subject area based on consultants subject matter expertise to: 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.

Balanced Risk Assessment

Ser.	Risk	Likelihood L/M/H	Impact L/M/H	Key Solutions / Mitigations (with others being identified in this DPIA)	Residual Risk	MPS SIRO Sign-Off
1.	The data entered into the RFR System is not treated within the correct Government Protective Marking Scheme (GPMS).	L	L	All MPS staff/ officers are trained in respect of the GPMS. Those using the RFR system will perform this task in a secure environment to which the public do not have access.		Lindsey Chiswick
2.	The RFR system contains inaccurate data that may lead to an unwarranted intervention by the police adversely affecting the rights and freedom of that individual.	M	M	Careful consideration of issues prior to the authorisation of an Image Reference Library for RFR Searching. The MPS upholds the rights of individuals under the DPA 2018. The MPS has policies and procedures that help to ensure that inaccurate information can be updated. This includes the MPS Privacy Notice, which provides measures that allow the public to correct inaccurate information that may be held about them.		Lindsey Chiswick
3.	The data generated by the RFR system is unlawfully disclosed to third parties.	L	H	Officers/Staff using RFR have been informed that this sensitive data must not be disclosed outside those with a need to know, and technical support staff. Any action following a Verified Match may involve the MPS working with other police forces, law enforcement bodies and other agencies to assist the MPS in discharging its		Lindsey Chiswick

				common law policing powers. This action will not require the sharing of biometric data but may require the MPS to share personal data, as it would for any investigation, in accordance with the MPS's routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect the RFR system and the USB used to import the data into the RFR system.		
4.	The RFR system and personal data associated with it is not being correctly managed in respect of the DPA 2018	L	H	The MPS RFR Documents outline how data will be processed lawfully, fairly and transparently in a manner which is necessary and proportionate for the purposes of the Human Rights Act 1998 and the DPA 2018. This DPIA is part of the framework put in place by the MPS to ensure compliance with the DPA 2018. The MPS RFR Form 1 and MP RFR Form 2 provides a structured approval process for the use of Image Reference Libraries for RFR Searching. The use of the 'Levels' system supports this and also provides for the submission (and where necessary) approval for the use of Probe Images for RFR Searching.		Lindsey Chiswick
5.	The RFR equipment is not functioning correctly.	L	M	The technology has been trialled and tested by the MPS. NEC algorithms have also been evaluated by NIST and the MPS pays regard to these findings.		Lindsey Chiswick

6.	Incorrect Matches may lead to an unwarranted action by the police adversely affecting the rights and freedom of that individual.	H	L	The Adjudication process set out in the RFR Policy will be adhered to, which requires human verification of matches. Training is provided to address confirmation bias issues.		Lindsey Chiswick
9.	Retention periods are not complied with.	L	M	The RFR team run regular audits to ensure that all personal data relating to the RFR system is held in line with the stated retention periods. The retention periods have been designed to ensure that data is retained for the minimum time periods necessary for the MPS to proportionately achieve its law enforcement purposes.		Lindsey Chiswick
10.	An individual wants to complain, exercise their individual rights under the DPA 18 and/ or submit a FOIA request.	M	L	MPS's RFR website contains details relating to RFR including the MPS RFR Legal Mandate, MPS RFR Policy Document, MPS RFR Standard Operating Procedures and this DPIA. The MPS website also has dedicated sections relating to FOIA requests and right of access requests. The MPS privacy notice is also published online and advises the public how they may exercise their individual rights. This DPIA also considers how RFR has the potential to impact individual rights and sets out appropriate mitigations to ensure such rights are upheld.		Lindsey Chiswick

12.	Misinformation within the public, impacting upon trust and confidence in respect of RFR	H	H	A stakeholder engagement strategy has been developed and is in place. Press and media strategies have been developed. Risk management strategies have additionally been developed in respect of this parameter.		Lindsey Chiswick

Implementation of DPIA Outcomes Responsibilities

	Action to be taken	Date for completion of actions	Responsibility for action
1.			
2.			
3.			
4.			

5. Conclusion

4.56 The DPIA has identified a number of relevant risks associated with the use of RFR.

4.57 Proportionate and reasonable mitigations have been identified and fall within the guidelines associated with the RFR operating principles. Whilst no exceptional areas of risk have been identified at present, this DPIA is a living MPS Document and as such will be subject to continuous review.

4.58 This DPIA complies with the requirements of Sections 35 – 40 and 64 of the DPA 2018.

Data Protection Impact Assessment Sign-off

DPIA Signature

1.	**Project Sponsor**
	Sign Below: Lindsey Chiswick
	Name: Lindsey Chiswick
	Position: Director of Intelligence
	Date: 25.08.2023
2.	**Data Protection Officer** I have been involved in and consulted as regards the development of FR policies and technologies over a number of years and have enjoyed an open channel of dialogue with the SRO throughout that time. I am consulted regularly on matters pertaining to the use of the tactic from the point of philosophical consideration of use through to active deployment. This particular DPIA relates Retrospective FR and in making comment formally, I have reviewed the Legal Mandate, Policy document and relevant RFR forms. Having done so, I am content that comprehensive consideration has been given to the prevailing privacy issues. In particular I note with regard to the use of custody images I note the detailed framework fettering the use of custody images to balance the gravity of the operational imperative with the risk of processing over-held imagery. Moreover, the wider sensitivity to the use of children's' images of various ages, again balanced against the operational imperative and severity of historic offending as an indicator of future risk. These approaches in my view seek to strike a reasonable balance between the necessity of acting and the protective rights which might otherwise be enjoyed. I have also considered the U16 MOPI 3 CONNECT Cohort Issue and can rationalise why the SRO has chosen the inclusion of this set notwithstanding that it means that a relatively small number of young peoples' images that would ideally have been set aside will potentially be processed for a limited time in the greater interests of protecting the public. Having considered the comprehensive nature of the documentation delivering controls over the use of RFR, I am satisfied that there are no residual high risks to rights and freedoms which have not been mitigated. That said, this is a new use of technology and I would therefore expect that deployments are closely monitored and any anomalies considered swiftly and reflected through an early review of this DPIA.
	Sign Below: Darren Curtis
	Name: Darren Curtis

	Position: DPO
	Date: 18.08.2023

Distribution List

Recipient	Title	Location

Change control:

Version	Date	Authority	Evidence of approval	Record of change

Appendix A – Glossary

Term	Acronym	Description
Data Controller		Has the same meaning as in section 1(1) of the DPA 2018, that is, the person who determines the manner in which and purposes for which Personal Data is or is to be processed either alone, jointly or in common with other persons
Data Protection Act 2018	DPA	Includes all codes of practice and subordinate legislation made under the DPA 2018 from time to time
Data Subject		Has the same meaning as in section 1(1) of the DPA 2018 being an individual who is the subject of Personal Data
Freedom of Information Act 2000	FOIA	Includes the Environmental Information Regulations 2004 and any other subordinate legislation made under FOIA from time to time as well as all codes of practice
Human Rights Act 2018	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes Personal and Special Category Data, Non-personal Information and De-personalised Information. May be used interchangeably with 'Data'.
Information Commissioner's Office	ICO	The independent regulator appointed by the Crown who is responsible for enforcing the provisions of the DPA 2018 and FOIA
Metropolitan Police Service	MPS	The police force for the London metropolis area (excluding the City of London)
Pseudonymous		Information that has never referred to an individual and cannot be connected to an individual.
Notification		The Data Controller's entry in the register maintained by the Information Commissioner pursuant to section 19 of the DPA 2018.
Process		Has the same meaning as in section 1(1) of the DPA 2018 and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying Personal Data

Personal Data		Personal data is information relating to a living identified or identifiable individual
Special Category Data		Special category data is information relating to racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards.

Protective Marking

Classification	Official
Suitable for Publication	Yes
Title	DPIA relating to the use of Retrospective Facial Recognition by the MPS.
Purpose	To cover privacy issues and mitigate risks arising from the use of Retrospective Facial Recognition technology.
Author	MPS RFR
Version	1.0
Creating Unit	MPS RFR
Date Created	01st August 2023
Review Date	18th August 2024
CYC Ref	