More Trust | Less Crime | High Standards

Classification	Official
Suitable for Publication	Yes
Title	MPS Appropriate Policy Document: Retrospective Facial Recognition (RFR) System
Purpose	Policy to outline the MPS's governance and compliance against Section 42 Data Protection Act 2018
Author	MPS RFR
Version	1.0
Creating Unit	MPS RFR
Date Created	24th August 2023
Review Date	24th August 2024

MPS Appropriate Policy Document: Retrospective Facial Recognition System

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

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

Sensitive processing is defined in Part 3 section 35(8) DPA 2018 and is equivalent to GDPR special category data. This includes:

a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE

purposes must be lawful and fair. Given RFR involves the processing of biometric data, section 35(5) requires this processing to be lawful and fair. The processing is only to occur where it is strictly necessary for the LE purpose and is based on a Schedule 8 condition. The MPS RFR Documents explain how this is achieved.

This document and the wider MPS RFR Documents together demonstrate that the MPS's processing of sensitive data in respect of RFR is compliant with the requirements within Part 3, Section 42 of the DPA 2018. In compliance with Section 42(2) of the DPA 2018 it explains the procedures and measures for securing compliance with the LE data protection principles and explains the policies as regards retention and erasure of personal data.

This document should be treated as being complimentary to the MPS general record of processing under S61 DPA 2018 and the MPS RFR Documents. It also complements the MPS' policy on protecting special category and criminal convictions policy.

Description of data processed - the data created by the RFR system

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 identify 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:

- the Templating of Probe Images produces personal biometric data; and
- the Templating of images on Image Reference Libraries being searched against Probe Images also produces personal biometric data.

Description of data processed - the data used by the RFR system

This will consist of a gallery of images (be it single capture or a frame extracted from media) or a short video against which Probe Images can be searched by the RFR System in order to seek Potential Matches (the Image Reference Library). A Temporary Image Reference Library can also be created for a discrete purpose linked to a specific investigation or operation.

The source of the Probe Images will depend on the nature of the searching being undertaken, but typically at the outset, it is expected to be from unsolved crimes, although it may also be drawn from other lawfully held images. 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 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.

Level, frequency of data being processed and the individuals impacted

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	Those on an Image Reference Library	Those subject to a Verified Match
Biometric Processing	**Yes**	**Yes**

Level of data being processed	Those on an Image Reference Library	Those subject to a Verified Match
	Biometric Templates are created for those on an Image Reference Library as part of the ingestion of the library into the RFR System.	Biometric Templates are created when an image is submitted for searching and becomes a Probe Image.
Imagery	**Yes**	**Yes**
	The image uploaded to the Image Reference Library is available to officers following a Potential Match so as to enable Adjudication.	The Probe Image uploaded to the Image Reference Library is available to officers following a Potential Match so as to enable Adjudication.
Personal data (such as name, date of birth, address)	**Uncertain**	**Uncertain**
	The extent of the personal data will depend on the Image Reference Library being searched.	The extent of the personal data will depend on the amount of data held in connection with the image. Where the Probe Image is of an unidentified suspect, this information will not be held.
Metadata	**Yes**	**Yes**
	In relation to the images uploaded to the Image Reference Library.	In relation to those matched on the RFR system.

Data is processed in relation to a specific RFR Search. A Probe Image would typically searched once, and then may also be submitted for further daily searching as part of the Unresolved Crime Cache against updates to the Custody Images Dataset. Submission to the Unresolved Crime Cache will be made with the authorisation of an officer of inspecting rank (or equivalent) or above, where there is a heightened level of intrusion. Images within the Unresolved Crime Cache will be subject to review every three, six or nine months (in accordance with the RFR Policy).

The number of people on an Image Reference Library / Temporary Image Reference Library will vary depending on the library. The Custody Images Dataset contains approximately 1m images and will be available for RFR Searching at the point the system goes live. Any other Image Reference Libraries to be made subject to RFR Searching will need to be approved in accordance with the RFR Policy.

The MPS RFR Policy outlines the criteria for images that may be considered appropriate for use on an Image Reference Library / Temporary Image Reference Library. The MPS RFR Policy also outlines considerations as to the source of an image that may be used on an Image Reference Library / Temporary Image Reference Library, noting that some imagery may engage greater privacy expectations than others. These controls assist the public and decision-making officers to understand RFR and how it may be used.

Data storage and review

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.

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

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

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.

(e) Additional safeguards, taking account of the increased intensity of the processing, are set out relating to the Custody Images Dataset, as set out in the RFR DPIA.

The right to request data erasure

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 needs to be retained is deleted by default. 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 utility of maintaining the Image Reference Library as resource for RFR Searching will also be 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 of the DPIA.

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 places to facilitate such requests.

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 MPS 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.

Data sharing

Should the RFR system generate a Potential Match, the subsequent process would typically also involve MPS personnel using policing databases and other intelligence systems 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.

Consent or Schedule 8 condition for processing

It is not practical to obtain consent of all data subjects whose data is processed in relation to the use of RFR. The MPS relies on there being a strict necessity to process the data for its LE purposes. The MPS also relies on Schedule 8. Whilst the Authorising Officer (AO) will confirm the Schedule 8 ground being relied on as part of the authorisation process permitting an Image Reference Library to be made available for RFR Searching, this will typically be that the use of RFR is necessary for judicial and statutory purposes – for reasons of substantial public interest. This is further explained in the MPS RFR Documents.

The Accountability principles

The MPS has in place appropriate technical and organisational measures to meet the requirements of the accountability principle. These include:

- data protection policies and other documentation which in the context of RFR include the MPS RFR Legal Mandate, MPS RFR DPIA, the MPS Privacy Notice, the MPS' policy on protecting special category and criminal convictions policy and the other MPS RFR Documents;
- detailed security measures relating to the RFR System;
- maintaining logs in relation to the RFR System in relation to decision making and Alerts – as further detailed in the MPS RFR Policy;
- data protection measures and policies to record and, where necessary, report personal data breaches;
- the appointment of a Data Protection Officer (DPO);
- responding to guidance and documentation produced by the Surveillance Camera Commissioner, the Biometrics Commissioner and the Information Commissioner; *and*
- a process for ongoing review, both post-search and in relation to the MPS RFR Documents. The DPO also has oversight of this via the MPS RFR Strategic Board.

Principle 1: Lawfulness and fairness

<u>The lawfulness of the MPS's use of RFR</u>: The MPS RFR Legal Mandate outlines:

- the legal basis on which RFR may be used by the MPS;
- the grounds when RFR may be used on the basis that it is strictly necessary for a LE purpose;
- confirmation that a condition of schedule 8 will be met;
- the safeguards and mitigations relating to data processing, human rights considerations; and
- how the MPS upholds the Public Sector Equality Duty.

The MPS RFR Policy and the MPS RFR Legal Mandate in particular provides detailed guidance to AO's on their responsibilities when considering if an Image Reference Library is appropriate for RFR Searching and is lawful and strictly necessary. This includes consideration of (i) what other policing methods have been used / discounted prior to using RFR, (ii) the importance of achieving the LE

purpose and the prospective of achieving it through the use of RFR (iii) the size and scale of the proposed RFR search and (iv) if the LE purpose which would underpin the use of RFR is strictly necessary and proportionate (not just desirable) to the need to undertake special category data processing and the risk to individual's rights. Individual Probe Images are also subject to an approval process prior to submission for RFR Searching.

The fairness of the MPS's use of RFR: The MPS Legal Mandate and the other MPS RFR Documents also explains how the MPS processes data fairly. Fairness is particularly relevant in two respects:

- Accessibility and foreseeability: The MPS RFR Documents are a control that regulates the discretion the police have to use facial recognition technology under its common law powers. By publishing these documents online, they are available to the public in a way that is accessible them. The documents also allows the MPS's use of RFR to be foreseeable to the public. The objective here is that the public should be able to read the documents and understand them. It should allow the public to anticipate how the MPS will use RFR and the policing need RFR allows the MPS to address. For example the Image Reference Library criteria in the MPS RFR Policy allows the public to understand the circumstances when an image may be considered for inclusion on an Image Reference Library.
- Fairness 'by design': 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 working with the National Physical Laboratory on the testing of the RFR System. That testing showing the RFR System was 100% statistically accurate.

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

- 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 by reviewing all alerts, including any incorrect ones 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's Facial Recognition Strategic Board which reviews the performance of the RFR system at a strategic level.
- Control measures to ensure fairness: the MPS will use the statistical reports produced by the RFR system that report on demographic issues. RFR Users will have training to ensure the RFR system is used compliantly and that retention protocols are followed.

Making available appropriate privacy information: 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. The MPS RFR Documents provide details about how:

- the RFR system will be used and
- the MPS will ensure the public are aware regarding how their personal data is processed in relation to RFR.

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. This is an important measure to inform Londoners including those who may be placed on an Image Reference

Library as to 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 where RFR may be used, and the considerations and constraints relevant as to who may be placed on an RFR Image Reference Library. 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 Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Protection of Freedoms Act 2012 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.
The Metropolitan Police Service Facial	• Explains in a public-facing summary: o how to understand RFR system accuracy;

Key documents available to the public	Information included
Recognition Technology: Understanding accuracy and demographic differences	• what the MPS have done to understand its algorithm within an operational context, including commissioning the NPL Study.
MPS RFR EIA	• Explains the MPS's approach to its responsibilities in relation to the Public Sector Equality Duty.

Principle 2: Purpose limitation

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

As the use of RFR is an investigative one, the officer commissioning the search is required to be satisfied with the legitimate aim and the legal basis for the usage of the RFR system. Key considerations relating to necessity and proportionality are addressed as part of the authorisation process. As noted above, before an Image Reference Library is made subject to searching it also requires an authorisation which take account of the necessity and proportionality of that searching.

The MPS RFR Legal Mandate also outlines MPS law enforcement purposes that can lawfully apply to justify the use of RFR. The MPS RFR Documents provide a structure to ensure that data is only processed for the authorised LE purpose.

Should a further LE purpose be identified after the AO has authorised an RFR Searching of an Image Reference Library, processing in respect of the further LE purpose is not permissible unless the AO provides an authority that covers the further law enforcement purpose and considers the need for a further Data Protection Impact Assessment.

RFR searches will be subject to monitoring and audit to ensure that the RFR system and its operation remains necessary, proportionate and effective in meeting its use case.

Principle 3: Data minimisation

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

Application & Authorisation

The RFR Application process adopted by the MPS in respect of Image Reference Libraries requires applicants to consider and demonstrate necessity of searching the library.

The AO needs to be satisfied that the use of the RFR system is necessary to the standards required by the Human Rights Act 1998 and the DPA 2018 in relation to biometric processing. This process also provides that any proposed processing that does not satisfy the necessity threshold should be challenged and not authorised.

Each subsequent RFR Search of a relevant Image Reference Library will require consideration and approval by the officer / staff member requesting the search or undertaking the search will also need to consider the necessity and proportionality of the search of a specific Probe Image. Searching of Probe Images Collections (where there are commonality between the images) may also be approved. The level of authorisation required for a Probe Image search will depend on a number of factors, including (by way of examples the suspected age of the data subject featured in the image and whether there are any grounds for elevated expectations of privacy. In such cases the Probe Image search request will require authorisation from a person of inspecting rank (or equivalent) or above.

Relevance

Those requesting/undertaking/approving a RFR Search need to consider the relevance of the Image Reference Library to their RFR Search Requirements and ensure searches against Image Reference Libraries relevant to the policing need are undertaken. By way of example, there would be little point in searching an Image Reference Library based on custody images if it is already established that the person of interest has not previously been detained by the police.

Adjudication

Adjudication means that the decision to determine if there is a Viable Match is made by an officer /staff and not the RFR system. As previously explained, officers will use their training and experience when deciding if there is a Viable Match. Approved users will also assess information from the RFR system – the Potential Matches are returned in rank number with the lower number first. If required, the list of candidates may be ordered by Match number and descending first. Any Potential Match is not a definitive result, and is merely presented to the RFR User for their consideration.

Ongoing accuracy

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.

Data Retention

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

1. 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.

2. 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.

3. 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.

Principle 4 Accurate and up to date

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, 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 the statistical accuracy and accuracy of personal data. These are set out below.

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).

Currency of Probe Image

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 4, 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.

Suitability for matching of the Image Reference Library

'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.

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.

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.

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.

Principle 5: Data is kept for no longer than necessary

The information will be retained in line with the MPS Retention, Review and Deletion Policy and the MPS RFR Documents. These are subject to at least annual review.

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 that 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 of the DPIA. 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.

Principle 6: Data security

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.

<u>Further Measures</u>

Include the following features:

a) The solution is hosted in the MPS' Azure secure environment;
b) Users have to logon to MPS which is then passed onto RFR via SSO;
c) Role based access conditions will limit the functionality available and access to data, enforcing the principles of least privilege and need-to-know
d) Azure leveraged security products including Prometheus and Grafana, Azure Security Centre, and Qualys.
e) All traffic will traverse existing Azure Expressway connections, it will not pass over the internet and is encrypted at rest and in transit (HTTPS).
f) Logging, alerting and auditing will be in place and supported by the relevant MPS tower.
g) An SDLC process will be in place to ensure artefacts received by suppliers are free from security vulnerabilities

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.

The MPS undertakes vetting checks on its personnel appropriate to their role.

The MPS RFR Documents and other relevant documents such as those relating to information security are subject of regular review.

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.