More Trust | Less Crime | High Standards

Classification	Official
Suitable for Publication	Yes
Title	Appropriate Policy Document for sensitive data processing within Live Facial Recognition deployments
Purpose	Policy to outline the MPS's governance and compliance against Section 42 Data Protection Act 2018
Author	MPS LFR
Version	2.0
Creating Unit	MPS LFR
Date Created	20th March 2023
Review Date	20th March 2024

MPS Appropriate Policy Document: Live Facial Recognition

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

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) 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 Live Facial Recognition 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 LFR Documents explain how this is achieved.

This document and the wider MPS LFR Documents together demonstrate that the MPS's processing of sensitive data in respect of live facial recognition technology (LFR) is compliant with the requirements with 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 LFR Documents. It also complements the MPS' policy on protecting special category and criminal convictions policy.

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

Biometric data: LFR 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. Where the LFR system identifies a potential image match, the LFR system flags an Alert to a trained member of MPS personnel who then makes a decision as to whether any further action is required. The LFR system therefore creates biometric data in two ways:

- the Templating of images of those included on a Watchlist produces personal biometric data; *and*
- the Templating of facial images from passers-by also produces personal biometric data for each face detected by the LFR cameras.

Other Personal Data**:** The use of LFR technology involves the creation of personal data. This includes the CCTV feed from the LFR system. It also includes metadata such as the time and location that people pass through the LFR system. Personal data (such as a person's name) may also be obtained as part of the Engagement process.

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

A bespoke Watchlist is imported into the LFR system for each Deployment. As well as including images of those being sought, it includes their name, date of birth, the date and location where the image was taken and the reason why they are of interest to the MPS. This data is handled in accordance with MOPI, in line with the MPS's wider policies on managing police data.

The data is typically drawn from the electronic warrants management system (EWMS), MPS custody and PNC. 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.

Level, frequency of data being processed and the individuals impacted

The below table summarises the key points during an LFR Deployment 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 a Watchlist	Those Engaged as a result of an Alert	Everyone who passes the LFR system
Biometric Processing	**Yes**	**Yes**	**Yes**
	Biometric Templates are created for those on a Watchlist.	Biometric Templates are created for those passing the LFR system.	Biometric Templates are created for those passing the LFR system.
Imagery	**Yes**	**Yes**	**Yes**
	The image uploaded to the Watchlist is available to officers following an Alert.	An image of the individual passing the LFR system is available to officers following an Alert.	The CCTV feed from the LFR deployment is recorded.
Criminal convictions data	**Yes**	**Yes**	**No**
	The reason why a person is being sought by the MPS is available to an officer following an Alert.	Personal data may be obtained - based on a policing need to verify an Alert.	
Personal data (such as name, date of birth, address)	**Yes**	**Yes**	**No**
	The details of the person being sought by the MPS is available to an officer following an Alert.	Personal data may be obtained - based on a policing need to verify an Alert.	
Metadata	**Yes**	**Yes**	**Yes**
	In relation to the images uploaded to the Watchlist.	In relation to those passing the LFR system.	In relation to those passing the LFR system.

Data is processed in relation to a specific LFR Deployment, the frequency of LFR Deployments being based on the intelligence case causing it to be necessary and proportionate to use LFR in furtherance of the MPS's common law policing powers and the availability of resource.

The number of people on a Watchlist will vary between Deployments. Rather than being driven by the LFR system's capacity, the inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality. The number of people on a Watchlist will therefore need to be as small as possible, whilst still achieving a legitimate policing purpose.

The number of people passing an LFR system will also vary between Deployments. Factors such as the time of day, Deployment length, nearby facilities, infrastructure, and public events will all influence the footfall expected to pass an LFR system. The MPS LFR SOP outlines the criteria for images that may be considered appropriate for use on a Watchlist. The MPS LFR SOP also outlines considerations as to the source of an image that may be used on a Watchlist, noting that some imagery may engage greater privacy expectations than others. These controls assist the public and decision-making officers to understand LFR and how it may be used.

Geographical scope

LFR will be used for a limited time, with a limited footprint, with a limited purpose of seeking to locate those whose presence is of justifiable interest to the MPS. Whilst LFR may be used at locations across London, any Deployment will be limited to a specific location using hardwired cameras linked to the LFR system. The locations used will be based on the intelligence case to Deploy LFR, the requirements of the LFR system and considerations relating to privacy that may attach to a particular area (as more particularly outlined in the MPS LFR Legal Mandate an the MPS LFR SOP).

Data storage and review

Data storage on the LFR system: The LFR system is a fully closed system with two layers of password protection to access the application. The LFR system is physically protected when in use and securely wiped following each Deployment. Access to the LFR system is limited to those with a need to use it.

Importing onto the LFR system: Images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine. Access to the USB stick containing the Watchlist is limited to those with a need to use it.

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 data held on the MPS systems is not specific to LFR (it provides LFR with the information needed to compile and generate a Watchlist and relates to policing information generated following LFR Alerts). 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 LFR Documents provide that:

- where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*
- the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:

- personal data is retained in accordance with the DPA 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
- personal data is retained beyond the 31 day period in accordance with the MPS's complaints / conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or*
- in accordance with the MPS's complaints / conduct investigation policies; *and/or*
- in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

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 LFR but applicable to all personal data processed by the MPS. LFR therefore does not restrict this right – in fact, the data created by LFR which no longer needs to be retained is deleted by default. This includes:

- where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; and
- the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable and in any case, within 24 hours following the conclusion of the Deployment.

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 LFR 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.

Watchlist data

The LFR Operator has the ability to delete images from the Watchlist and will record such action in their log. This may be necessary when a valid request for erasure is received. It may also be necessary if a person was validly placed on a Watchlist at the point the Watchlist was imported into the LFR system but was subsequently located by LFR and dealt with by the MPS before passing the same LFR Deployment later in the day. In these circumstances and to mitigate against future Alerts being generated, the image may be removed by the Operator from the Watchlist.

Data sharing

Should the LFR system generate an Alert, 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 LFR. 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 will confirm the Schedule 8 ground being relied on as part of the authorisation process, this will typically be that the Deployment of LFR is necessary for judicial and statutory purposes – for reasons of substantial public interest. This is further explained in the MPS LFR Documents, particularly the MPS LFR Legal Mandate.

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 LFR include the MPS LFR Legal Mandate, the MPS LFR DPIA, the MPS Privacy Notice, the MPS' policy on protecting special category and criminal convictions policy and the other MPS LFR Documents;
- detailed security measures relating to the LFR system;
- a 'data protection by design and default' approach to the LFR system which includes the deletion of the biometric data of those who are Templated by the LFR system on entering the Zone of Recognition but do not trigger an Alert;
- maintaining logs in relation to the LFR system in relation to decision making and Alerts – as further detailed in the MPS LFR SOP;
- data protection measures and policies to record and, where necessary, report personal data breaches;
- the appointment of a data protection officer;
- 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-Deployment and in relation to the MPS LFR Documents. The Data Protection Officer (DPO) also has oversight of this via the MPS LFR Strategic Board.

Principle 1: Lawfulness and fairness

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

- the legal basis on which LFR may be used by the MPS;
- the grounds when LFR 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 LFR SOP and the MPS LFR Legal Mandate in particular provides detailed guidance to Authorising Officers on their responsibilities when considering if the Deployment of an LFR system is lawful and strictly necessary. This includes consideration of (i) what other policing methods have been used / discounted prior to using LFR, (ii) the importance of achieving the LE purpose and the prospective of achieving it through the use of LFR (iii) the size and scale of the proposed LFR Deployment and (iv) if the LE purpose which would underpin the use of LFR is strictly necessary and proportionate (not just desirable) to the need to undertake special category data processing and the risk to individual's rights.

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

- Accessibility and foreseeability: The MPS LFR 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. Together with the MPS's commitment to give prior notification of its Deployments, the documents also allows the MPS's use of LFR to 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 LFR and the policing need LFR allows the MPS to address. For example the Watchlist image criteria in the MPS LFR SOP allows the public to understand the circumstances when an image may be considered for inclusion on a Watchlist.
- Fairness 'by design': The MPS has published a paper entitled 'Understanding the Metropolitan Police Service LFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its LFR algorithm.

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 LFR Documents already provide for ongoing evaluation and a post-deployment review process for LFR Deployments on a per Deployment basis. 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 LFR system at a strategic level.
- Training to ensure fairness: The MPS LFR Documents provide that officers and staff involved with an LFR Deployment will receive training. This is beneficial to ensuring fairness, particularly during the Adjudication Process. During this process, when an officer is deciding whether to Engage a member of the public, police officers are required to exercise their own judgement based on their training and experience. The training includes ensuring officers understand the characteristics of the LFR system that could affect the likelihood that an Alert is reliable – this specific training has a number of purposes including helping guard against the assumption that because an Alert has been generated it may be assumed to be correct. Police officers and staff also receive training to on discrimination and bring this knowledge to bear when discharging their duties.

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 LFR, the MPS has adopted a number of measures to ensure that the right to be informed is upheld. The MPS LFR Documents provide details about how:

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

This includes the use of prominent signage, leaflets and officers assisting the public during a Deployment. It will also include the use of the MPS's online channels to make the public aware of the use and results on LFR.

A key measure is the publication of the MPS Privacy Notice, the MPS policy on protecting special category and criminal convictions, and key MPS LFR 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 the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the Metropolitan Police Service (MPS), as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist. In this way, the MPS's use of LFR 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 LFR Legal Mandate	• The lawful basis for processing data in relation to LFR. 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

Key documents available to the public	Information included
MPS Policy Document	• An outline, strategic intent and objectives for the use of LFR and how personal data will be used by the LFR system • Key terms used across the MPS LFR Documents • Data retention periods applicable to LFR
MPS LFR Standard Operating Procedure Processes	• Outlines measures relevant to considering where LFR can be Deployed by the MPS. • Watchlist considerations including the basis on which images may be added to a Watchlist and considerations relevant to the sources of non-police originated imagery. • Provides that during any policing operation where LFR is Deployed officers will be available to assist member of the public with queries, and: o signs publicising the use of the technology must be prominently placed in advance (outside) of the Zone of Recognition; and o any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. • Both of these measures will be easy to read and together will ensure those passing the LFR system/who are Engaged by it will have the opportunity to seek further information. Both the signs and leaflets will provide an accessible QR code and website link to the MPS website for more information.
MPS LFR 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 LFR 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 LFR System's Accuracy and Bias Position	• Explains in a public-facing summary: o how to understand LFR system accuracy; o what the MPS have done to understand its algorithm within an operational context.
MPS LFR 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 LFR is an operational one, the AO is required to be satisfied with the legitimate aim and the legal basis for the Deployment. Key considerations relating to necessity and proportionality are addressed in depth as part of the authorisation process.

The MPS LFR Legal Mandate also outlines MPS law enforcement purposes that can lawfully apply to justify the use of LFR. The law enforcement purpose for each Deployment will be articulated and authorised by the AO within the Written Authority Document. The MPS LFR Documents provide a structure to ensure that data is only processed for the authorised law enforcement purpose.

Should a further law enforcement purpose be identified after the AO has authorised an LFR Deployment, processing in respect of the further law enforcement purpose is not permissible unless the AO provides an authority that covers the further law enforcement purpose. Such authority would consider the lawfulness, strict necessity and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.

LFR Deployments will be subject to regular review to ensure that the LFR system and its operation remains necessary, proportionate and effective in meeting its use case.

Principle 3: Data minimisation

The MPS LFR 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.

<u>Application & Authorisation</u>

The LFR Application process adopted by the MPS requires applicants to consider and demonstrate necessity in considerable detail. Once this and other stages are satisfactorily completed, the Application then progresses into the Authorisation phase, where a senior MPS police officer (the Authorising Officer) considers necessity as part of any authority they provide for the use of LFR.

The AO needs to be satisfied that the Deployment is necessary to the standards required by the Human Rights Act 1998 and Data Protection Act 2018 in relation to biometric processing. This process makes clear that the need to use LFR should not be merely desirable, but is needed to meet a law enforcement purpose. This process also provides that any proposed processing that does not satisfy the necessity threshold should be challenged and not authorised.

By way of example, the AO must be satisfied by the steps taken to ensure that composition of a Watchlist is not excessive, and only includes those who need to be located by the MPS using LFR, on a strict necessity basis.

<u>Ongoing Review</u>

The MPS LFR Documents require that on an ongoing basis, the Gold and Silver Commanders review the Deployment to ensure that it continues to meet the strict necessity threshold, and the requirements of proportionality. The Gold and Silver Commanders are obligated to stop the Deployment at any point, should the Deployment fail to meet the requirements of this Data

Protection Principle (amongst other reasons). The LFR Operator is also required to ensure that the LFR system is correctly working and will advise the Silver Commander should they identify any issues.

Relevance

There are a number of requirements that help to ensure the Deployment is relevant to its legitimate aim and to ensure the relevance of the data being processed. These include:-

1. the need for a Deployments, and the location of the Deployment to be supported by intelligence and other policing information to confirm the need for the Deployment and the prospects for locating those sought;

2. the inclusion of an individual(s) on a Watchlist is to be:

    a. supported by intelligence or other information which supports the need to locate these individuals (such as a court warrant having been issued for their arrest); *and*

    b. a policing decision is made as to the prospects of locating them through the use of LFR.

3. the selection of images for an LFR Watchlist requires the MPS to lawfully hold them, and the MPS to have undertaken reasonable measures to ensure that the image selected is accurate such that it could be expected to assist with locating an individual of interest to the MPS;

4. the LFR system reviews images submitted for inclusion on a Watchlist and will flag issues where the image may not be suitable; *and*

5. the Threshold can be adjusted for an Alert on the LFR system to set an appropriate tolerance to avoid unduly triggering False Alerts.

Adjudication

Adjudication means that the decision to Engage a member of the public is made by an officer and not the LFR system. As previously explained, officers will use their training and experience when deciding whether an Engagement is required. Officers will also assess information from the LFR system taking account of Environmental, Subject and System Factors that may affect the likelihood that an LFR Alert means that the subject is the same person held on the Watchlist. When considering generating an Alert image for officers to review, the LFR system 'by design' automatically obscures the faces of others in that image who are not the subject of an Alert. This approach limits the level of processing where an Engagement does not occur and helps ensure relevance where it does.

Ongoing Watchlist accuracy

The LFR Operator has the ability to delete images from the Watchlist and will record such action in their log. This may be necessary if a person was validly placed on a Watchlist at the point the Watchlist was imported into the LFR system but was subsequently located by LFR and dealt with by the MPS before passing the same LFR Deployment later in the day. In these circumstances and to mitigate against future Alerts being generated, the image may be removed by the Operator from

the Watchlist. In any event, the Adjudication process and the role of the Engagement Officer and LFR Operator mitigates against the likelihood of Engaging once again with that person.

Data Retention

Controls have been implemented to minimise impact on the wider public and those on Watchlists. The controls provide that:-

1. where the LFR system does not generate an Alert, a person's biometric data is immediately automatically deleted; *and*

2. the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:-

1. personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*

2. personal data is retained beyond the 31 day period in accordance with the MPS's complaints / conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*

2. in accordance with the MPS's complaints / conduct investigation policies; *and/or*

3. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Technical systems and standard operating procedures help ensure that data is properly retained or deleted. A post-Deployment review process and associated internal audit function provides assurance in this regard.

Processing mechanisms, LFR policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes

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 LFR] 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 LFR system at the outset, including evaluating claims made by the vendor. In this respect the MPS has paid close regard to the NIST findings. The MPS has published a paper entitled 'Understanding the Metropolitan Police Service LFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its LFR algorithm. In relation to NIST, this paper notes:

> *"The Met's facial recognition system uses an algorithm from a leading vendor, NEC. The NIST Test report published in 2018[1] evaluated over 200 algorithms for their accuracy. Its findings state that:*
>
> > *"NEC, which had produced broadly the most accurate algorithms in 2010, 2013, submitted algorithms that are substantially more accurate than their June 2018 versions and on many measures are now the most accurate"."*
>
> *"In March 2017, NIST also published a Face In Video Evaluation (FIVE) report.[2] Unlike the other NIST Tests, the FIVE test involved the use of video footage as opposed to static images. This is of particular interest to the Met because this aligns more closely to the Met's use of facial recognition in a 'live' - video context. The NEC algorithm was found to be the most accurate across the different measures with a True Positive Identification rate of 82% at a corresponding False Positive Identification Rate of 0.4%."*

The ICO has also highlighted the importance of implementing monitoring, the frequency of which should be proportional to the impact an incorrect output may have on individuals. The higher the impact the more frequently it is that monitoring and reporting is required. Cognisant of this ongoing process, the MPS LFR Documents already provide for ongoing evaluation and a post-deployment review process for LFR Deployments on a per Deployment basis. 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 LFR system at a strategic level.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf
[2] https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

Currency of Watchlist

The MPS LFR Documents provide that Watchlists uploaded to the LFR system will not be more than 24 hours old. This helps to provide increased assurance that those on Watchlists remain of interest to the MPS.

Where it has been identified that it is appropriate to add an individual to a Watchlist, technical measures are in place to cross reference data with the PNC to verify that these persons are still of interest to the MPS prior to the encrypted transfer of a Watchlist to the LFR system. 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 as part of an LFR Deployment.

Accuracy of Watchlist

A new Watchlist is generated for every LFR Deployment. This is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching. MPS personnel are required to have taken reasonable steps to ensure that the image is of a person intended for inclusion on a given Watchlist. Images on a Watchlist will be lawfully held by the MPS. In respect of custody images, the MPS has an explicit statutory power to acquire, retain and use such imagery (see s.64A Police and Criminal Evidence Act 1984).

Where a change to data is reported by a data subject, where possible this will be used to update the LFR system and used to avoid the data subject making multiple reports.

Quality of Watchlist Images

The MPS LFR Documents provide guidance in relation to which images are to be considered appropriate for inclusion on an LFR Watchlist. When an image is added to a Watchlist, the LFR system assesses image quality and suitability for matching, in order to allow MPS personnel to consider and manage the risk that poor quality images might generate False Alerts.

Distinguishing Data Subjects

The LFR system produces a Template for everyone who enters the Zone of Recognition when their face is successfully detected by the system. It is not relevant or possible to distinguish between people subject of processing as a result of their being in the Zone of Recognition.

In relation to those on a Watchlist, when an Alert is generated, the system makes data available to the System Operator and Engagement Officers regarding the Watchlist subject linked to the Alert. This data includes relevant details about why the subject is on a Watchlist, e.g. wanted by the MPS for rape. This allows Engagement Officers to distinguish between those categories of person identified in s.38 (3) DPA (where applicable) and this will help inform their action.

The Engagement Process

The Engagement process provides an opportunity for Engagement Officers to speak with members of the public and does not automatically result in the use of any policing powers.

The process provides opportunity for Engagement Officers to consider the policing data associated with a person on a Watchlist. Where lawful, the officer is able to undertake further checks to verify the information they have, helping ascertain its continued currency and accuracy.

MPS Policy

The MPS upholds the rights of individuals under the DPA. 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 LFR Documents. These are subject to at least annual review.

MPS LFR Documents detail specific controls relating to LFR data retention. The controls help ensure that the only data retained, is that which is strictly necessary to meet the purpose of the Deployment. The controls provide that:-

1. where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*

2. the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable and in any case, within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 31 days, except where:

1. personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and/or

2. personal data is retained accordance with the MPS's complaints/conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and /or*

2. in accordance with the MPS's complaints / conduct investigation policies; *and/or*

3. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Principle 6: Data security

The LFR system includes a number of physical and technical security measures. These include:

1. images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine; *and*

2. the LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data; *and*

3. that the system is physically protected when in use and securely wiped following each Deployment; *and*

4. that role based access controls with limited user permissions are been implemented on the system; *and*

5. that the LFR application is connected to mobile devices using a private access point with three levels of protection; Specific IP addressing, password access to the access point, and password access to the mobile App. The mobile App has a RESTful API and will be covered by SSL; *and*

6. that the Dashboard and RESTful API are secured with SSL and TLS by default; *and*

7. that all connections are directed through HTTPS; *and*

8. that a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*

9. that technical issues with the LFR system are always dealt with by LFR System Engineers working on the Deployment.

Further Measures

As a contingency against the LFR system failing in some way that requires the LFR Operator to wipe and reset it, the encrypted USB memory stick containing the Watchlist is retained with the LFR Operator until the end of the Deployment. This means that the LFR Operator is able to reimport the Watchlist to the rebooted LFR system, enabling the Deployment to continue.

The MPS LFR Documents outlines the actions that must be taken in the event that personal data is lost. The LFR 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 LFR Documents and other relevant documents such as those relating to information security are subject of regular review.

Security Against Unlawful Processing

The MPS LFR Documents set out the structures that enable and support lawful authorisation of LFR Deployments by the MPS. No Deployment is permitted without that authorisation. During

Deployment, command teams are required to monitor and review data processing to ensure that it remains lawful. A post-Deployment debrief and review is used to identify lessons for the future and periodic audit provides assurance.