DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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

1.7 This document is designed to be used as an overarching DPIA to support the deployment of LFR by the MPS. Prior to any Deployment this DPIA should be reviewed and amended where necessary before being adopted as a DPIA to cover a specific Deployment or set of Deployments. Adopted DPIAs will contain similar wording across key areas with amendments made where necessary to reflect any specific characteristics of a Watchlist or a Deployment.

1.8 This document should be read in conjunction with the MPS LFR Documents.

Role of the Data Protection Officer

1.9 <u>Pre-Deployment Planning:</u> For those involved in the review, amendment (as necessary) and adoption of a DPIA for a specific Deployment or set of Deployments, there is a need to engage with the Data Office before the DPIA is submitted to the Data Protection Officer (DPO) for sign-off.

1.10 The roles of the DPO and the Data Office are an important part of the process in the pre-Deployment planning stage of any LFR Deployment. 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 MPS Commissioner. The fact that the DPO is an independent body provides further assurance. The DPO's involvement in the pre-Deployment planning process is evidenced by their sign-off of the overarching DPIA for LFR and any Deployment-specific DPIA.

1.11 **Colleagues are encouraged to make early contact with the Data Office mailbox when planning an LFR Deployment.**

1.12 Post-Deployment Review: The DPO and Data Office's role continues throughout the LFR Deployment – acting as points of contact and providing means of ongoing assurance in relation to data processing queries. They also facilitate data subjects to exercise their individual rights. The post-Deployment Review also presents an opportunity to engage with the DPO and Data Office where trends or concerns are identified. Within the MPS the senior internal oversight body for LFR is the MPS FR Technology Board, which in turn answers to the MPS Management Board. The DPO sits on the MPS FR Technology Board and as such is able to retain oversight on the conduct of LFR Deployments.

2 Data Protection and Data Processing

Purpose of the processing

Purpose of LFR

LFR technology is an operational tactic that helps the MPS stop dangerous people who are wanted for criminal offences. It helps keep Londoners safe.

As a police service, the MPS has a number of long-established policing responsibilities and powers derived from the common law which have been consistently recognised by the courts. The MPS is obliged to comply with the common law and statutory safeguards in delivering its policing operational duties, and relies on the common law to discharge a number of its duties. LFR can assist with the MPS's duties to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security. This includes targeting those wanted for imprisonable offences, with a focus on serious crime, including paying particular regard to knife and gun crime, child sexual exploitation and terrorism. It also includes using LFR technology to protect the public, reduce serious crime and help safeguard vulnerable persons.

The MPS's objectives for LFR are further outlined in the MPS LFR Documents, particularly Chapter 5 of the LFR Guidance Document.

Benefits of LFR

The MPS has drawn extensively on the experience gained from the LFR trials to inform the future use of LFR. The MPS view is that LFR is a valuable tool that supports the MPS in keeping London safe for everyone. The MPS trials have shown the potential benefits of LFR as an important policing tool – its use has resulted in the arrest of wanted individuals. The MPS LFR trials demonstrate that LFR technology can significantly improve the effectiveness of an officer's ability to locate wanted individuals. It can assist officers where traditional policing methods may struggle to yield results. An individual officer cannot possibly remember all of the faces of wanted persons on a Watchlist. Neither can an individual officer easily spot someone in a large crowd. LFR is a tool that improves the MPS's chances of picking out the person it is looking for.

LFR has a number of advantages over other systems currently used by the MPS, such as CCTV. LFR allows the MPS to deploy its resources more efficiently. For example, the LFR system will actively alert officers to the potential presence of individuals of interest to them rather than requiring larger numbers of officers to watch a busy CCTV feed. LFR has the capacity to assist officers where the number of people passing officers (or a CCTV system) makes identifications challenging (e.g. when the number of individuals to be identified is significant).

LFR also has a public protection and safeguarding role. For example, where the courts have issued a warrant for a person's arrest, many of these people pose a risk to public safety. These people may be located using LFR in circumstances where the officers would otherwise struggle, and could not possibly be expected to remember the faces of all those currently wanted by the courts. The *Bridges* judgments recognised this rationale and supports this use case.

The ongoing effectiveness of the MPS's use of LFR is reviewed by way of the post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander, and address the efficiency and efficacy of the Deployment.

LFR's benefits are further outlined in the MPS LFR Documents, particularly Chapter 4 of the MPS LFR Guidance Document and Section 3 of the MPS LFR Legal Mandate.

Context of the processing

Relationship to individuals

LFR relates to individuals in three ways (1) those on an LFR Watchlist (2) those passing the LFR system and (3) protecting the public more generally.

Watchlist: The Deployment of LFR is driven by MPS policing priorities and intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose which determine the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, and that need fits with the policing purpose driving the LFR Deployment. This may include those aged under 18, those under 13, a person with a disability (as defined in the MPS LFR SOP) or vulnerable adults where there is a policing need and it is deemed to be necessary and proportionate to locate and/or safeguard these people. The MPS LFR Documents outline considerations regarding expectations of privacy, and outlines specific controls and safeguards to mitigate any impact on those with a protected characteristic(s).

Whilst the upper size of the Watchlist may be a limiting factor on occasion (where the necessity and proportionality case has been made out for more people than it is possible to add to a Watchlist), this is anticipated to be a very rare occurrence. It is also crucial to note that the technical potential size of a Watchlist does not drive Watchlist composition in any way – intelligence, locality and policing purposes and policing priority do in line with the MPS's strategic objectives as set out in the MPS LFR documents. Together, they may justify the necessity and proportionality of the particular Watchlist's composition and the need to Deploy LFR using a Watchlist designed for the needs of that Deployment.

Passing the LFR system: LFR works by analysing key facial features of those passing the LFR system to generate a mathematical representation of them. This involves the processing of biometric data given the need to create Templates of everyone who passes the LFR system and compare them to those held on a Watchlist.

The courts have recognised the right of the police to make use of a photograph of an individual. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect's accomplice, or of anyone else. The court confirmed the "key is that they must have these and only these purposes in mind and must … make no more than reasonable use of the picture in seeking to accomplish them". Additionally, as the Surveillance Camera Code notes, an individual can, however, "rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place". The position in relation to LFR was considered in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin).* The court recognised in that case the policing common law powers to use facial recognition technology were "amply sufficient" and that biometric processing of passers-by, whilst fleeting in nature, would be on the grounds of strict necessity to fulfil a law enforcement purpose as opposed to being based on consent. The position was further considered by the Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058.* The Court of Appeal concluded:

> *"The short answer, in our view, to this submission is that the legal framework which regulates the deployment of AFR Locate does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary."*

Consent would be entirely impractical to obtain during an LFR deployment, and would undermine the law enforcement purpose underpinning the Deployment.
The Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058* confirmed the Division Court's general findings on the legal framework but further noted that, to be 'in accordance with the law' the legal basis must:

> *"be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself".*

In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held in the case before it to determine *where* they deployed facial recognition technology and *who* they deployed it to locate those on a Watchlist. The court refers to this as the "Where Question" and the "Who Question".

(a) The 'Where Question: The MPS LFR Documents answers this question, particularly the MPS LFR SOP at Section 5. In answering this question, in many instances, the need to locate a person will determine where it is best to site LFR to facilitate making a successful location. However, other factors will also be relevant and these include the nature of the site itself from a privacy perspective, those passing the site, and the policing need to be at the site (including for the public's protection).

(b) The 'Who' Question: the MPS addresses the 'Who Question' in its published MPS LFR Documents, particularly at Section 6 of the MPS LFR SOP. The MPS sets the criteria that applies to govern the images that may be included on a Watchlist and in what circumstances. To ensure the Watchlisting criteria is accessible and foreseeable, the MPS explains terminology such as 'presenting a risk of harm' and 'victims, persons with information and close associates' to ensure that these are readily understood and objective to both officers and the public. It sets out the standard required for inclusion on a Watchlist, linking the necessity and criteria for the inclusion on a Watchlist with the policing need and the proportionality of taking any action.

Public protection: LFR has the potential to engage the wider public, not just those passing the LFR system. Whilst the wider public that do not pass the LFR system will not be engaged by having their personal data processed, the effective use of LFR to locate those wanted by the MPS and the courts serves wider public protection and safeguarding purposes. This is all the more evident when necessity and proportionally is considered as part of the process of adding people to a

Watchlist. There is therefore a substantial public interest in enabling the MPS to efficiently locate those wanted by it.

<u>Technology</u>

LFR is a relatively new technology in a law enforcement context. However it is increasingly common-place with a growing number of applications beyond law enforcement and within law enforcement itself. It is also a technology that has been trialled and tested by the MPS in order to understand its utility as a policing tool.

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) 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. 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, including undertaking a process of peer review. 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%."*
>
> *"When considering 'bias' (or demographic differentials as it is more accurately referred to), the first thing to measure is the overall system accuracy and then establish if there is a statistically significant variation in that accuracy levels based on a person's demographic such as gender or ethnicity*
>
> *In 2019, NIST published the first study to assess whether demographics such as gender or ethnicity cause FR Identification system accuracy to vary.3 Tests were run on a 2.6 million image dataset where images were balanced with respect to representation of gender and ethnicity. The NIST results demonstrate that not all algorithms show uniform accuracy levels across the different demographics. However, NEC, the vendor used by the Met was found to perform well, with NIST saying that NEC had:*

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

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

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

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

The MPS LFR 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 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 Facial Recognition Technology Board.

Public perception and expectations

A number of bodies have undertaken surveys relating to public awareness and perceptions of LFR. These surveys help inform the MPS and its approach to LFR.

ICO: A report was commissioned by the ICO in January 2019 which indicated that there is strong public support for the use of LFR for law enforcement purposes:

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

The public’s support holds up even if they were to be stopped by the police as a result of LFR matching them (erroneously) to a subject of interest. 58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.

London Policing Ethics Panel (LPEP): LPEP is an independent body set up by Mayor to provide advice on ethics, who produced a report on the MPS trials of LFR. The report included the results of a survey undertaken by LPEP:

- 57% of those surveyed felt police use of LFR is acceptable;
- public support increases to 83% acceptance for LFR to search for serious offenders;
- 50% of those surveyed feel that the technology would make them feel safer; *and*
- approximately one third raised concerns about the impact on their privacy.

More widely the LPEP report outlined five conditions that they considered necessary to support the ethical use of LFR in a law enforcement context. The MPS has responded to the LPEP report and the five conditions proposed within it.

The LPEP report is here:
http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

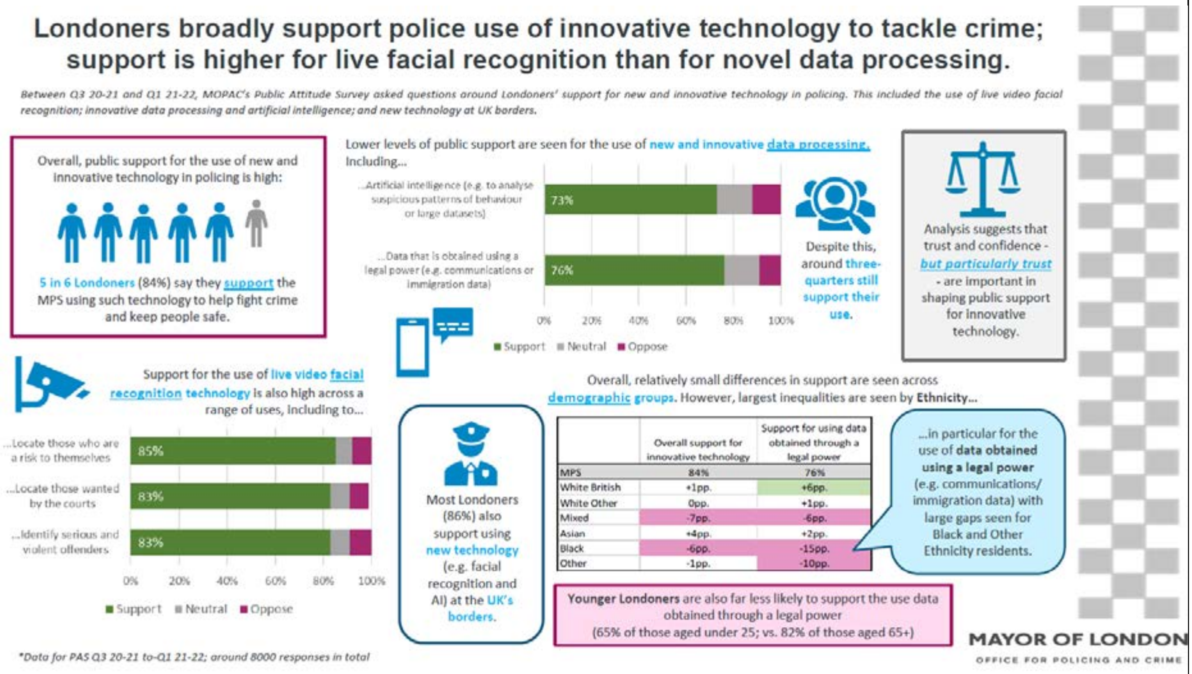
The MPS response to the LPEP report is here:
https://www.london.gov.uk/sites/default/files/mayor_of_london_-_lfr.pdf

MOPAC Public Attitudes Survey:

In Q3 FY 20-21, 3,202 Londoners were asked to what extent they support or oppose the MPS using technological innovations in a range of situations. It concluded that public support for the MPS's use of innovative technology is high, but varies by age, ethnicity and broader attitudes towards the police. 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	**55+**	+4pp	+3pp	+4pp	+3pp	+2pp
Ethnicity	**White**	+1pp	+1pp	+3pp	0pp	0pp
	Mixed	-10pp	-1pp	-15pp	-12pp	-9pp
	Asian	+4pp	+2pp	+2pp	+6pp	+8pp
	Black	-6pp	-6pp	-10pp	-4pp	-6pp

The MOPAC Public Attitudes survey has continued to ask questions around Londoner's support for new and innovative technology in policing. The results of the PAS Q3 20-21 to Q1 21-22 survey findings, including those in relation to LFR follow:



Londoners broadly support police use of innovative technology to tackle crime; support is higher for live facial recognition than for novel data processing.

Between Q3 20-21 and Q1 21-22, MOPAC's Public Attitude Survey asked questions around Londoners' support for new and innovative technology in policing. This included the use of live video facial recognition; innovative data processing and artificial intelligence; and new technology at UK borders.

Overall, public support for the use of new and innovative technology in policing is high:

5 in 6 Londoners (84%) say they support the MPS using such technology to help fight crime and keep people safe.

Lower levels of public support are seen for the use of new and innovative data processing. Including...

...Artificial intelligence (e.g. to analyse suspicious patterns of behaviour or large datasets)
73%
...Data that is obtained using a legal power (e.g. communications or immigration data)
76%
0%
20%
40%
60%
80%
100%
Support
Neutral
Oppose

Despite this, around three-quarters still support their use.

Analysis suggests that trust and confidence - *but particularly trust* - are important in shaping public support for innovative technology.

Support for the use of live video facial recognition technology is also high across a range of uses, including to...

...Locate those who are a risk to themselves
85%
...Locate those wanted by the courts
83%
...Identify serious and violent offenders
83%
0%
20%
40%
60%
80%
100%
Support
Neutral
Oppose

Most Londoners (86%) also support using new technology (e.g. facial recognition and AI) at the UK's borders.

Overall, relatively small differences in support are seen across demographic groups. However, largest inequalities are seen by **Ethnicity**...

	Overall support for innovative technology	Support for using data obtained through a legal power
MPS	84%	76%
White British	+1pp.	+6pp.
White Other	0pp.	+1pp.
Mixed	-7pp.	-6pp.
Asian	+4pp.	+2pp.
Black	-6pp.	-15pp.
Other	-1pp.	-10pp.

...in particular for the use of **data obtained using a legal power** (e.g. communications/ immigration data) with large gaps seen for Black and Other Ethnicity residents.

Younger Londoners are also far less likely to support the use data obtained through a legal power (65% of those aged under 25; vs. 82% of those aged 65+)

**Data for PAS Q3 20-21 to-Q1 21-22; around 8000 responses in total*

MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

The role of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner

Whilst the MPS would welcome and wish to be part of any process to produce a code of conduct for the use of algorithm-based technologies, the MPS has paid close regard to the detailed legal framework identified in the *Bridges* decisions. It is also responsive to the views expressed by the various regulators. The MPS has paid regard to the ICO and the opinions issued by the Information Commissioner in relation to facial recognition technologies. Cognisant of their role in relation to regulating the use of surveillance cameras and their use in conjunction with LFR technology the MPS has also considered the Surveillance Camera Code and the guidance 'Facing the Camera'. LFR deployments include the use of the Surveillance Camera Commissioner's Check-list.

Nature of the processing

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.

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.

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 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.

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.

High risk processing

Innovative Technology: Whilst LFR is relatively new to law enforcement, the technology has been specifically designed for facial recognition. In order to operate LFR effectively, the MPS has run a trial programme before any operational use to inform its future use and to ensure the effectiveness of the overarching safeguards adopted by the MPS LFR Documents.

Biometric Data: The LFR system processes biometric data, both in relation to those on a Watchlist and those passing an LFR system. Security measures including safeguards 'by design' have been identified and implemented in this DPIA and the MPS LFR Documents to mitigate risk in relation to biometric data processing.

Data Matching: 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. The Adjudication process requiring human-in-the-loop decision making, and other mitigants have been identified and implemented in this DPIA and the MPS LFR Documents.

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 LFR Documents and this DPIA and is not considered to be high risk as a result.

Scope of the processing

Nature of the data

In order to generate Alerts, the LFR system 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.

The Templates of those on the Watchlist can then be compared to the Templates of those passing the LFR system. An Alert is generated when the similarity between the Templates exceeds the Threshold.

Officers consider Alerts during the Adjudication process and then make a decision as to whether any further action is required. This further action may include an Engagement with a member of the public. As part of this process officers will have access to the data associated with the image on the Watchlist. This includes that person's name, date of birth, the date and location where the image was taken and the reason why they are of interest to the MPS. As part of the Engagement process personal data may be obtained (such as a person’s name, date of birth and address) to assists officers in confirming the validity of an Alert.

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

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 might 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 foresee how it may be used.

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.

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 and the MPS LFR SOP). These controls assist the public and decision-making officers to understand LFR and foresee where it may be used.

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	Live Facial Recognition involves the real-time searching of facial images from a video stream, against a Watchlist, in order to produce an immediate search result that generates an Alert when a likely match is found. The submission of Probe Images is triggered by passers-by entering the LFR Zone of Recognition with their faces visible to an LFR camera. Human input is required to determine the likelihood that an Alert is accurate and whether any policing response is required.		
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 LFR 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	Every face of a passer-by that is detected by the LFR system will be Templated to allow the LFR system to determine whether an Alert should be triggered to indicate a potential match with a Watchlist image.		
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	LFR is a relatively new technology to UK Law Enforcement.		
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 LFR does not involve DNA samples, DNA profiles and/or fingerprints, the LFR 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 Watchlists may use data that comes from a number of sources, all images submitted for inclusion on a Watchlist must 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). The decision to place a person on a Watchlist and the Deployment of LFR will include the use of policing databases and other intelligence systems.		

	Should an Alert be generated, 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.		
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 LFR system is a closed system which does not involve the tracking of an individual's online or offline location or behaviour. It does however allow MPS personnel to locate persons of interest to the MPS at a point in time when they pass through the Zone of Recognition. LFR's ability to provide a location at a single point in time may assist the MPS to continue to locate an individual over a period of time. This would occur when LFR is used in a coordinated manner with a variety of policing tools, which together combine to allow the MPS to continue to locate an individual. For example LFR may be combined with on-street CCTV systems that continue to confirm where an individual is located.		
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 LFR system involves the processing of biometric data relating to subjects and includes data outlining the reasons why the MPS wishes to locate them. Both categories are further considered below: Biometric data is recognised by the DPA 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 LFR 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 Watchlist will be determined by the policing need, in line with the MPS LFR Documents. Many thousands of faces of passers-by may be (momentarily) Templated during the course of a LFR Deployment.		
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 Deployments are overt and include prominent signage and details regarding the use of LFR via the MPS's online channels. The provision of individual privacy notice personally to each person passing the LFR system would be impractical.		
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 LFR system processes all detected faces regardless of 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 Watchlist image.		

4 Data Protection and 'Privacy Law' Assessment

European Convention of Human Rights
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

The MPS LFR Legal Mandate for the use of LFR provides detailed analysis relating to Article 8 and other legal considerations relevant to the use of LFR.

Accountability

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

Home Office Biometric Strategy Published June 2018

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:

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

1. protect life and property;

2. preserve order and prevent threats to public security;

3. prevent and detect crime;

4. bring offenders to justice;

5. uphold national security.

Article 8 recognises action in the interests of national security, public safety, the prevention of disorder or crime as legitimate aims. The use of LFR in the context of fighting crime including knife and gun crime, child sexual abuse and exploitation (including online), and terrorism offences will help the MPS to achieve its law enforcement purposes.

Any Deployment of LFR needs to meet a 'Pressing Social Need'. How a specific LFR Deployment satisfies this requirement is outlined in this DPIA, the MPS LFR Documents and will be documented and authorised on a Deployment-by-Deployment basis via the Written Authority Document process. In this regard the following Statutory Instrument passed in the context of the Data Protection Act 1998 is informative.

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?

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

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 LFR. These safeguards are set out below.

The LFR Application process adopted by the MPS requires applicants to consider and demonstrate proportionality in considerable detail. Once this and other stages are satisfactorily completed, the Written Authority Document process then requires a senior MPS police officer (the Authorising Officer) to consider proportionality as part of any authority they provide for the use of LFR. These processes have been adopted as they mirror those used to grant RIPA authorities, where internal and external scrutiny has demonstrated their value.

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, then a person's biometric data is immediately automatically deleted;

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.
   .

Public Awareness

Deployments do not constitute `covert surveillance' as defined by s.26(9)(a) of the Regulation of Investigatory Powers Act 2000. The MPS LFR Documents outline a number of measures adopted by the MPS to ensure that the public are aware of a LFR Deployment (via signage, leaflets and the MPS's online information channels).

Watchlist Creation

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).

The LFR system assesses images for quality and suitability. This ensures that only those of a good enough standard are used for matching, thus allowing MPS personnel to consider and manage the risk of poor quality images generating inaccurate LFR matches.

Specific measures are outlined in the MPS LFR Documents governing the inclusion of persons aged under 18 on a Watchlist. This means that inclusion is considered on a case-by-case basis. Specific legal advice and input from subject matter experts is required before an image of a child (who appears to be) aged under 13 years old[4], a person with a disability (as defined in the MPS LFR SOP at paragraph 6.6), and in relation to gender reassignment (as outlined in the MPS LFR SOP at paragraphs 6.3 – 6.7) can be included. Such inclusions require the specific authority from the AO.

Appropriate LFR Technology

As technology continues to improve, the MPS will continue to review its LFR capability to ensure that performance is maximised, that intrusion is minimised, and to ensure that Deployments remain proportionate whilst achieving their 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.

The MPS LFR Documents also outline points relating to the LFR system to ensure that it is used in a way that maximises its effectiveness. They also place responsibility on the Silver Commander and LFR Operator to continually monitor and review the system's performance.

Technical and Security Measures

All staff employed on MPS LFR Deployments will be security vetted MPS employees.

Appropriate technical and organisational measures will be in place to safeguard against unauthorised loss, disclosure or destruction of data used for the operation (e.g. uploaded facial images), and to ensure that it is retained when necessary (e.g. recorded positive matches).

These measures are further outlined within the LFR MPS LFR Documents.

Officer Policing Experience

There is a well-established legal basis whereby officers may ask questions of members of the public. LFR as a policing tool does not change the core policing role or necessarily result in any disadvantage when an Engagement occurs. LFR is not a means of identification in itself. However, LFR does provide information to officers that helps officers select persons they may wish to Engage with. LFR does not alter the principle that an officer still needs to decide whether they speak to a member of the public or not.

When deciding whether to Engage a member of the public, police officers are required to exercise their own judgement based on their training and experience. Officers should do this in exactly the same way they would when receiving any other piece of information, for example where a photo circulated to officers of a wanted suspect or a description of a possible offender provided to officers over their police radio. Relying on training, experience, and where necessary assistance from colleagues helps ensure that the right decisions are made about when, where and how to

[4] Generally, studies [https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf] have shown that young children, up to the age of 13 are both harder to correctly recognise (lower True Positive Identification Rate) but also harder to distinguish between (higher FPIR). The higher FPIR may lead to more False Alerts being generated against young children if there is an image of a young person in the Watchlist.

members of the public are approached. Only where an officer makes a decision to approach a member of the public may that officer then take steps to confirm their identity in accordance with their policing powers.

Adjudication

When the LFR system generates an Alert, it is not an automatic consequence that any member of the public will be Engaged by the MPS. This means that even if those passing the LFR system generate an Alert, it does necessarily not follow that those people will be Engaged.

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 has provided an accurate identification. Ultimately, no Engagement will be made unless an officer is content that there is (i) a lawful basis to support the policing need to engage with the individual, and (ii) the engagement is necessary and proportionate in the circumstances.

Furthermore, even when an Engagement occurs, this in itself does not mean that any further police action beyond the Engagement will result. Officers require a legal basis to support any action taken.

Authorisation and Review Process

The MPS LFR Documents detail how the MPS use of LFR technology is authorised, managed and reviewed post-Deployment. The processes help ensure that the use of LFR is limited in terms of duration, operational footprint, its purpose, and how it impacts on human rights and the level of data processing undertaken.

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.

Consideration of Alternative Policing Tools

The use of LFR as a tool to locate persons of interest to 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.

Training

The MPS LFR Documents provide for the training of officers and staff involved in an LFR Deployment. The training helps ensure role specific:

1. familiarity with the MPS LFR Documents;

2. knowledge of Deployment processes;

3. understanding of the lawful processing of personal data in accordance with the Data Protection Act 2018;

4. understanding the scope of the Regulation of Investigatory Power Act 2000;

5. knowledge of police powers and how they may apply when responding to Alerts;

6. knowledge of how to configure the LFR system to maximise system performance, and how to minimise impact on others;

7. understanding of the characteristics of the LFR system that affect the likelihood that an Alert is reliable.

Adjusting the Threshold

If during Deployment a Watchlist image generates more than one False Alert, then consideration will be given to raising the Threshold for Alerts for that Watchlist subject. More generally, the MPS SRO for LFR has directed that the False Alert Rate should be kept within a 1 in 1000 level to minimise the impact on the passing public whilst balancing the policing need to locate those on a Watchlist.

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.

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 LFR Legal Mandate.

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.

The MPS LFR Legal Mandate outlines:

1. the legal basis on which LFR may be used by the MPS;

2. the grounds required where LFR may be used on the basis that it is strictly necessary for a law enforcement purpose;

3. confirmation that a condition of Schedule 8 will be met;

4. how the MPS upholds the Public Sector Equality Duty.

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 allow the MPS's use of LFR 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 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. This document recognises a position of high performance such that the MPS has confidence it can achieve its legitimate aims but, in line with the ongoing nature of the legal duties on the MPS, it notes:

  > *The NIST Tests can only take the Met so far, and by their nature, factors relevant to an operational environment can only be realistically tested with real-life operational use. Further controlled testing would not accurately reflect operational conditions, particularly the numbers of people who need to pass the LFR system in a way that is necessary to provide the Met with further assurance.*

To that end the Met have tested and continue to test NEC algorithms under operational conditions.

- To this end, the MPS has an action plan that continues to support operationally realistic testing to build on its position with target timelines:

Stage	Process	What is invovled	Targeted timeline
1	Review large scale trials conducted on NEC algorithm to baseline equitability performance	The MPS's Understanding Accuracy and Bias document details diligence to date and strong algorithm performance but now recommends operational testing specific to use-cases in line with the MPS's continuing PSED responsibilities.	**Complete** – Review when new version of algorithm released
2	Review scientific literature with regards best practice for measuring equitability	NIST & ISO documents consulted & submission for STAR funding to support Equitability testing of Live Facial Recognition Technology	**Complete**
3	Write outline Equitability test approach	Work with a range of experts to define a scientifically robust test methodology to measure equitability testing in an operational Live Facial Recognition context	Prior to Deployment 1
4	Assess safeguards	Assess wider safeguards for operational use against updated governance documents. Review & Feedback to operational use	Deployments 1 & 2
5	Undertake discovery process and refine test methodology	Undertake discovery process to ensure test methodology is feasible. Review & Feedback to test methodology, operational use & safeguards	Deployments 1 & 2
6	Data Collection & Testing	Collect test cohort and trial data. Analyse & review outcomes.	Deployments 3 -7
7	Report Findings	Write report on System Equitability for Live Facial Recognition. Peer Review & revision.	Post Deployment 7 + 3 months
8	Human Factors	Further research to understand Human Factors with respect to end to end Facial Recognition Technology	Ongoing
9	Data Curation	Curate data to support future testing of FR technologies to ensure ongoing commitment to PSED	Ongoing
10	Review	Continuously review operational outcomes and effectiveness. Review when Facial Recognition Algorithm is updated	Ongoing

<u>Additionally, in relation to fairness, the MPS has also taken the following measures:</u>

- <u>Ongoing reviews to mitigate risks of unfairness</u>: 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 FR Technology Board that 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.

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.

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.

Within the context of a LFR Deployment, the MPS’s approach to the management of the Watchlist, in particular segregation between categories on the overall Watchlist also embeds the processing of personal data for specified, explicit and legitimate purposes. By ensuring technical measures are adopted through the segregation within the Watchlist this ensures the status of those on a Watchlist will be recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated. This helps uphold the purpose limitation and ensures that an Alert results in suitable, calibrated response honed to the legitimate purpose of processing the data.
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.

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.

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.

Application & Authorisation

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.

Ongoing Review

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.

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

All personal data processing will be strictly necessary and proportionate to the legitimate aim of the relevant Deployment.

The MPS has carefully evaluated the personal data to be used during the LFR Deployment 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 LFR system. As an example, when calculating the number of people who have passed through the Zone of Recognition, instead of retaining Templates and using those at a later point in time, the assessment is carried out manually by an officer or member of staff determining the flow-rate at different points during the Deployment.

Data Protection Act 2018 - Principle 4

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

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 LFR 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.

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[5] 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.[6] 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

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

[6] https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

to explore that further and test for issues under the oversight and scrutiny of the MPS's FR Technology Board that reviews the performance of the LFR system at a strategic level.

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 are, and 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. The MPS SOP recognises that there may be a need to adjust the Threshold to ensure that the False Alert remains within the 1:1000 level determined by the MPS SRO and empowers the LFR Operator to monitor for issues of LFR system performance, flagging these to the Silver Commander.

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.

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.

Yes. The LFR system software automatically and immediately deletes any biometric data that does not generate an Alert against the Watchlist. 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?

MPS personnel will take all reasonable steps to ensure that each image included on a Watchlist does actually pertain to the intended person. When adding an image to a Watchlist, the LFR 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 LFR 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 LFR Documents. These are subject to at least annual review.

What retention periods are suitable for the personal data the MPS will be processing?

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.

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.

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

1. that images are transferred to the LFR system via an encrypted USB, that is further protected by pass number access; *and*

2. that the LFR system is a fully-closed system with multiple layers of password protection to access the application; *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 mandates base-line data protection training for all personnel – “Information and you”. This is therefore a pre-requisite to participate in a LFR Deployment.

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.

Safeguards - Archiving

Personal and special category data shall be processed where the processing is necessary for archiving purposes in the public interest.

Refer to section **5. Balanced Risk Assessment** below. Schedule 8 conditions will apply to LFR 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.

Refer to section **5. Balanced Risk Assessment** below. Schedule 8 conditions will apply to LFR 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 (DPO).

Complaints about the use of Personal Information in relation to this project should be handled through the Data Office triage team overseen by the MPS Data Protection Officer (DPO).

Freedom of Information Act 2000 (FoIA)

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.

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.

In accordance with guidance from the ICO, the MPS will place this DPIA and other associated MPS LFR 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.

All public requests for information should be directed through the Data Office triage team overseen by the MPS DPO.

Individual Rights

Part 3, Chapter 3 of the Data Protection Act 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)

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.

5 Individual Rights

Data Protection Act 2018 – right to be informed

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.

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 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

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 typically 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 EIQ	• Explains the MPS's approach to its responsibilities in relation to the Public Sector Equality Duty.

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

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

Data Protection Act 2018 – right of access

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 LFR 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 Data Office to ensure the MPS complies with this legal obligation.

Data Protection Act 2018 – the right to rectification

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 on a Watchlist. The LFR Watchlist creation process draws on existing MPS data to produce the Watchlist allowing existing MPS processes to be used to enable data subjects to exercise their right of rectification.

Whilst this right is not specific to LFR but applicable to all personal data processed by the MPS, the process by which Watchlists are compiled have been implemented to ensure currency and accuracy in so far as it is possible to do so. The MPS LFR Documents provide that Watchlists uploaded to the LFR system will not be more than 24 hours old. Technical measures are in place to cross reference data with the PNC to verify that these persons are still of interest to the MPS and their data remains accurate prior to the encrypted transfer of a Watchlist to the LFR system.

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 how 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

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:

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.

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 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.

- **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.

Occasions when individual rights may be limited

In accordance with Section 48 of the Data Protection Act 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;
5. protect the rights and freedoms of others.

This is not a point that is specific to LFR 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

Part 3 of the Data Protection Act 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. it is based on automated processing; and

2. it produces an adverse legal effect or a significantly affects the individual.

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 LFR Deployments.

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 has provided an accurate identification. Ultimately, no Engagement will be made unless an officer is content that (i) there is a lawful basis to support the policing need to engage with the individual, and (ii) the engagement is necessary and proportionate in the circumstances.

6 Consultation Results

Stakeholder Engagement and Consultation

6.1 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 LFR. This has helped to shape the ongoing engagement and consultation process.

6.2 The engagement and consultation process has helped inform the MPS's understanding of how LFR 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.

6.3 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 Deployments, and as the MPS continues to review and learn from its LFR Deployments.

Stakeholders	**Roles and Responsibilities**	**Outcomes**
	Provision of guidance on completion of the DPIA and Pilot Exercise.	*Advice issued.*
Information Commissioner	Advice in relation to the DPIA.	ICO opinion
London Policing Ethics Panel	Recommendations.	Incorporated into governance documents.
Surveillance Camera Commissioner (Former)	Discussion linked to project proposals and implementation.	Compliance with SCC Code of Practice.
Defence Science and Technology Laboratory	Guidance on procurement, testing and Deployment of the technology, along with advice around academic research and literature supporting the proof-of-concept view of the product.	Engagement and consultation continues.
Home Office Biometric Programme	Additional guidance.	Engagement and consultation continues.
MOPAC	Early engagement linked to the concept, testing, implementation, and its impact on human rights (including privacy).	Engagement and consultation continues.
National Police Chiefs Council AFR VVIS Board (now the Facial Recognition Technology Board)	Discussion and advice linked to the development of the project and the use of custody images.	Support and consistency at a national level.

The Biometrics Commissioner (Former)	Discussion linked to project proposals and implementation.	Engagement and consultation continues.
The Biometrics and Surveillance Camera Commissioner	Discussion linked to facial recognition proposals and implementation.	Engagement and consultation continues.
The College of Policing	Discussion linked to Deployment of LFR and development of Approved Professional Practice.	Engagement and consultation continues.
Police ICT Company	Discussions linked to system developments and the benefits of developing a coherent and consistent application across the law enforcement community.	Engagement continues.
Essex University	Discussions linked to academic research into MPS use of LFR technology, and the ethical dilemmas associated with it.	Independent academic report.

Public Consultation

6.4 Retaining public confidence in the MPS to safeguard and process all (sensitive) personal data held is of paramount importance to the MPS. The MPS therefore has widely engaged and continues to engage with its stakeholders and the public informed by its trials and use of LFR to date.

6.5 A robust consultation strategy has ensured comprehensive feedback, commentary and support in the creating and quality control of the DPIA. The MPS welcomes any feedback on the use of the technology, and are very much aware of the ethical considerations and debates that exist around the use of LFR. To that end the MPS has ensured that details regarding the use of the technology, along with numerous potential use case scenarios have been presented to MOPAC and made available to the wider public. Wider debate has also been sought with the then Surveillance Camera Commissioner. Among others, representatives of Liberty and Big Brother Watch have accepted invitations to attend the MPS LFR trials. Concerns over its use have been raised by both representatives from Big Brother Watch and Liberty and these have been carefully considered. Time has also been made to discuss the use of the technology in more detail with representatives from Big Brother Watch and Liberty.

6.6 Local accountability is delivered through an established governance structure further outlined in the MPS LFR Guidance Document.

6.7 The operational imperative to deploy the technique as part of the control strategy for a high risk, high profile event has wherever possible involved the communities served by the MPS. Use of LFR has received widespread publicity through the communication strategy, advertising the tactic in advance of Deployment (throughout the trials). This approach has also assisted academic research, as the reception of the tactic will form part of the review to be undertaken in support of the use of technology. The communication strategy seeks to inform the public of the proposed use, its potential for impact on privacy and the proportionality of that impact as opposed to arguably more intrusive, traditional tactics.

6.8 As the use of LFR is developed, the below table will continue to be populated with some of the methods of continued consultation used by the MPS and the outcomes of the consultation.

	Date	Method of Consultation	Stakeholder	Outcomes
1.	2019 – January 2020	MPS intranet website, blogs, SPOC meetings and engagement sessions.	MPS	Enhanced awareness
2.	Issued/displayed at each deployment.	Leaflets / signage	Public	Enhanced awareness
3	2020 – Date	Further SPOC meetings and engagement with wider law enforcement	MPS / Wider Policing	Enhanced awareness

7 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 onto the Watchlist is not treated within the correct Government Protective Marking Scheme (GPMS).	L	L	All MPS staff/ officers are trained in respect of the GPMS. Officers compiling Watchlists will perform this task in a secure environment to which the public do not have access. All Watchlists are appropriately stored prior to the operation and are deleted after the Deployment.	L	Lindsey Chiswick
2.	The Watchlist contains inaccurate data that may lead to an unwarranted intervention by the police adversely affecting the rights and freedom of that individual.	M	M	Watchlists are bespoke to a Deployment. The MPS LFR Standard Operating Procedures provide that they should not be imported into the LFR system more than 24 hours prior to the start of the Deployment in order to ensure the Watchlist is current. 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. The technical team also review the Watchlist to ensure that the correct formatting/ inputting procedures have been followed to minimise the rate of False Alerts. 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. The Engagement process provides an opportunity for Engagement Officers to consider the policing data associated with a person on a Watchlist. Where lawful, the officer is able	L	Lindsey Chiswick

				to undertake further checks to verify the information they have, helping ascertain its continued currency and accuracy. 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.		
3.	The Watchlist or other data generated by the LFR system is unlawfully disclosed to third parties.	L	H	Officers/Staff compiling the Watchlists are briefed in respect of Watchlist circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff. Any action following an Alert may 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. Physical and technical security measures are in place (as described in this DPIA) to protect the LFR system and the USB used to import the data into the LFR system.	L	Lindsey Chiswick
4.	The LFR system and personal data associated with it is not being correctly managed in respect of the DPA 2018	L	H	The MPS LFR 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.	L	Lindsey Chiswick

				The MPS Form LFR 1 provides a structured application and approval process for any proposed LFR Deployment. This involves scrutiny by a senior police officer and allows the MPS to demonstrate compliance with the law on a Deployment-by-Deployment basis.		
5.	The LFR 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. An LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of false positives to below 0.1% will be present at all Deployments. All relevant information is logged for audit purposes. Logs are kept by the Gold, Silver and LFR Operator. The MPS LFR Documents also outline points relating to the LFR system to ensure that it is used in a way that maximises its effectiveness. They also place responsibility on the Silver Commander and LFR Operator to continually monitor and review the system's performance. The Gold and Silver Commanders are obligated to stop the Deployment, should the Deployment fail to meet the requirements of the DPA 2018 at any point. The ongoing effectiveness of the MPS's use of LFR is reviewed by way of the post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.	L	Lindsey Chiswick

6.	False Alerts may lead to an unwarranted intervention by the police adversely affecting the rights and freedom of that individual.	H	L	The Threshold for system Alerts is set sufficiently high so that less than 1 in a 1,000 passers-by will generate a False Alert. (The negative consequence of this is that subjects who are on the Watchlist are likely not to generate an Alert on approximately 25% of the occasions they enter the Zone of Recognition.) All images that result in a Watchlist Alert will additionally be reviewed by an Engagement Officer prior to engagement with the subject. Engagement Officers are trained to have regard to Subject, System and Environmental Factors. This will further increase the likelihood that the biometric match relates to the person whose details are held on the Watchlist. In the event that a subject is engaged due to a False Alert, the level of intrusion (if any) will usually be minimal as it will typically simply result in an officer speaking to the individual and confirming their identity.	L	Lindsey Chiswick
7.	An incorrect person is stopped by police as consequence of a correct Watchlist indication.	L	L	The LFR screen captures information of the upper torso, including clothing. This image is forwarded to the intervention officers via a secure IT link to a mobile device. The Engagement Officer therefore has a precise image of the person sought, negating the likelihood of an incorrect person being stopped.	L	Lindsey Chiswick
8.	An unlawful arrest is made	L	H	Officers are briefed prior to each Deployment and are informed LFR is a process that is only deployable in conjunction with human intervention. Once an Alert has been generated, officers will be tasked to intervene and use intelligence databases and interactions with the individual to confirm whether they are the same person as on the Watchlist.	L	Lindsey Chiswick
9.	Retention periods are not complied with.	L	M	The LFR team run regular audits to ensure that all personal data relating to the LFR system is held in line with the stated retention periods. The retention periods have been designed	L	Lindsey Chiswick

				to ensure that data is retained for the minimum time periods necessary for the MPS to proportionately achieve its law enforcement purposes. Where possible retention periods have been implemented ‘by design’. The main example of this is where the LFR system does not generate an Alert. In these circumstances a person’s biometric data is immediately automatically deleted.		
10.	An individual who has been stopped as a result of an LFR Alert wants to complain, exercise their individual rights under the DPA 18 and/ or submit a FOIA request.	M	L	Information leaflets are to be offered to those Engaged as a result of an LFR Alert. This information encourages stakeholder feedback and provides contact details. The command team will provide signposting for an LFR Deployment via large display screens/posters or other suitable means, advising that police are using cameras for LFR. All officers deployed on these operations are briefed in respect of the aims and objectives of the LFR system. They will be in a position to answer queries and can will be able to report any feedback to operational leads. MPS’s LFR website contains details relating to LFR including the MPS LFR Legal Mandate, MPS LFR Guidance Document, MPS LFR 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 LFR has the potential to impact individual rights and sets out appropriate mitigations to ensure such rights are upheld.	L	Lindsey Chiswick
11.	Watchlist data is disclosed following an LFR operation.	L	H	Procedures are in place to destroy data on LFR Watchlists after the operation has taken place. The data retention policy relating to LFR is detailed in the MPS LFR Documents and in this DPIA.	L	Lindsey Chiswick

12.	Misinformation within the public, impacting upon trust and confidence in respect of LFR	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. The MPS has undertaken to publish details relating to planned Deployments and the results of its Deployments online.	M	Lindsey Chiswick

8 Implementation of DPIA Outcomes Responsibilities

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

9 Conclusion

9.1 The DPIA has identified a number of relevant risks associated with the Watchlist compilation and security, operational Deployment of LFR and post-LFR Deployment phases.

9.2 Proportionate and reasonable mitigations have been identified and fall within the guidelines associated with the LFR 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.

9.3 A new DPIA will be produced as necessary for each Deployment.

9.4 The intelligence supporting Deployment will be incorporated within the intelligence case documented within the MPS Form LFR 1.

9.5 The overt nature of these Deployments will be highlighted through signage on the day, which will be prominently placed on the approach to the LFR cameras, outside the Zone of Recognition.

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

10 Data Protection Impact Assessment Sign-off

DPIA Signature

1.	**Project Sponsor**
	Sign Below: Lindsey Chiswick
	Name: Lindsey Chiswick
	Position: Director of Intelligence
	Date: 29th November 2021
2.	**Data Protection Officer**
	I have been involved throughout the lifecycle of the development of this DPIA and therefore its earlier iterations. The use of facial recognition has, in my view, been measured. It has drawn from learning elsewhere, and the MPS has applied a philosophy of rigorous testing; measured application; and continuous learning and improvement with an aspiration to be and remain 'best in class'. I am of the opinion that a depth of thought has been applied to identifying the classes of persons likely to be affected by the processing and has developed appropriate controls and safeguards where necessary to safeguard the rights and freedoms of individuals. This review demonstrates clearly that the aforementioned philosophy is in action. I remain entirely satisfied that this DPIA more than adequately describes the nature of processing envisaged, lawful basis, necessity, proportionality, controls and mitigations etc. I am content that the processing described does not present a high risk to the Rights and Freedoms of individuals. Darren Curtis
	Name: Darren Curtis
	Position: DPO
	Date: 30th November 2021

Distribution List

Recipient	Title	Location

Change control:

Version	Date	Authority	Evidence of approval	Record of change
2.0	29th Nov 2021	Director of Intelligence / DPO	Section 10	Changes to reflect updates to other documents and additional controls now possible for the Engagement process.

11 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.

12 Protective Marking

Classification	Official
Suitable for Publication	Yes
Title	DPIA relating to the use of Live Facial Recognition by the MPS.
Purpose	To cover privacy issues and mitigate risks arising from the Deployment of Live Facial Recognition.
Author	MPS LFR
Version	2.0
Creating Unit	MPS LFR
Date Created	29th November 2021
Review Date	29th November 2022