Protective marking:	Official
Publication scheme Y/N:	No
Title:	LIVE FACIAL RECOGNITION: LEGAL MANDATE
Version:	1-01
Summary:	Outlines the legal basis for the MPS's use of LFR technology
Branch/ OCU:	MPS DLS
Review date:	24/01/2021

MPS LIVE FACIAL RECOGNITION: LEGAL MANDATE

This legal mandate will be subject to periodic review, on at least an annual basis. It can be amended as the law and technology develops further, or as matters relating to Live Facial Recognition (LFR) evolve. It is anticipated that circumstances may arise which fall outside of the scope of this legal mandate. In such circumstances legal advice should be sought from the Directorate of Legal Services.

Terms & Definitions: Capitalised terms used within this LFR Legal Mandate shall have the meaning given to them in the MPS LFR Guidance Document unless otherwise defined in this LFR Legal Mandate.

1 Legal Mandate

1.1 LFR for law enforcement purposes is not subject to dedicated legislation. Instead, in line with the way the Metropolitan Police Service (MPS) exercises its well established common law powers, LFR is regulated by a number of sources of law, more particularly identified below. These sources of law combine to provide a multi-layered legal structure to use and regulate the use of LFR (the LFR Legal Framework).

Level One: Legislation	**Legal power to use LFR**	a) Common Law
	Regulating the use of LFR	<u>Operational</u> b) Human Rights Act 1998 c) Equality Act 2010 <u>Data Management</u> d) Data Protection Act 2018 (including the Law Enforcement Directive) e) Protection of Freedoms Act 2012
	Requests for information in relation to LFR	f) Freedom of Information Act 2000

Level Two: Code and Guidance	**Regulating the use of LFR**	a) Secretary of State's Surveillance Camera Code of Practice and associated guidance and other documentation issued by the Surveillance Camera Commissioner b) Information Commissioner's Office Code of Practice for Surveillance Cameras and associated guidance issued by the Information Commissioner

Level Three: MPS LFR Documents	**Regulating the use of LFR**	a) MPS Policy Documents b) MPS Standard Operating Procedures and Guidance Documents c) MPS Training Documents d) MPS Data Processing Appropriate Policy Document e) Data Protection Impact Assessment f) Equality Impact Assessment g) Community Impact Assessment h) LFR Risk Assessment

2 Common Law

2.1 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.

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

(a) protect life and property;
(b) preserve order and prevent threats to public security;
(c) prevent and detect crime;
(d) bring offenders to justice; *and*
(e) uphold national security.

Example: The MPS has identified uses for LFR as a tool for identifying those who have outstanding warrants for their arrest for knife and gun crimes. In this context, the use of LFR technology to facilitate officers to promptly locate those evading arrest would enable the MPS to discharge its responsibilities to protect life and property. It would also be compatible with the MPS's duty to bring offenders to justice by facilitating a prompt and effective investigation.

2.3 The use of the police's common law powers as a legal basis to support the use of LFR has been considered by the courts in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)* (the "Bridges" case). The court recognised the use of LFR Watchlists to identify those of "possible interest" to a police force for intelligence purposes as well as for the purposes of taking "all steps… necessary for keeping the peace, for preventing

crime or for protecting property". In this context the court recognised the police's common law powers to be "amply sufficient" and confirmed that "the police do not need new express statutory powers for this purpose".

Key point for Authorising Officers: When considering the use of LFR technology, MPS Authorising Officers should be clear as to the common law policing power the MPS relies on for lawful authority to use LFR and record this as part of the decision making process.

3 Human Rights Act 1998

3.1 All MPS use of LFR will be in compliance with the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

"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."

3.2 As a qualified right, any interference with an individual's Article 8 rights is only permissible if:
(a) there is a legal basis for the interference with the qualified right that the public can understand;
(b) the use of LFR seeks to achieve a legitimate aim;
(c) it is necessary for the purposes of that aim in a democratic society; *and*
(d) the use of LFR is proportionate to the legitimate aim being sought.

3.3 It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom*[1] confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that LFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".[2]

3.4 The *Bridges* case further considered Article 8, specifically in the context of facial recognition and has confirmed that Article 8 is engaged in so far as someone passes an LFR system and in so far as someone is placed on a LFR Watchlist for a Deployment. Depending on the nature of the Deployment, the Surveillance Camera Commissioner has identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. Authorising Officers should contact the Directorate of Legal Services should they consider a proposed Deployment may have wider human rights points to consider.

[1] *(2009) 48 EHRR 50, at [66 and 67]*
[2] *At [104]*

3.5 There is a legal basis for the interference with the qualified right that the public can understand.

LFR will be used to allow the MPS to discharge its well established operational duties pursuant to common law. The courts have recognised that "the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them".[3]

In the case of *R (Catt) v Chief Police Officers [2015] A.C. 1065,* Lord Sumption recognised that applicants could have their personal information noted down and retained by the police as they occupied publically accessible space. The court recognised the police's common law powers to collect and store information are subject to an "intensive regime of statutory and administrative regulation" under the Data Protection Act and various guidance documents on the management of police information.

The courts have further recognised the right of the police to make use of a photograph of an individual. The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. 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".[4]

In the case of the MPS's use of LFR, the LFR Legal Framework outlines the legal basis for any interference with an individual's Article 8 rights. The *Bridges* case has confirmed the police's common law policing powers to be "amply sufficient" in relation to this type of use of LFR. With the benefit of the *Bridge's* judgment, the law has now been applied to LFR. This judgment, taken together with the MPS's published documentation to support the use of LFR allows the LFR Legal Framework principles to be predictably applied to the use of LFR in an accessible and understandable way.

3.6 The use of LFR seeks to achieve a legitimate aim.

Article 8, recognises action in the interests of national security, public safety and 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.

Key point for Authorising Officers: At the point that it is decided to deploy LFR, the decision maker should be clear as to its purpose and how using LFR will help the MPS realise a legitimate aim. In deciding if the use of LFR is a suitable way to achieve a legitimate aim, the decision maker should consider if benefits of using LFR justify its use for that legitimate aim when compared to any impact on an individual's Article 8 Rights.

[3] R (*Catt) v Association of Chief Police Officers [2015] A.C. 1065* at [11].
[4] Per Laws J in *Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804 at 810F*

3.7 The use of LFR is *necessary* for the purposes of that legitimate aim in a democratic society

LFR will be used in response to a pressing social need by helping the MPS to fight crime in areas where LFR has the greatest potential to assist. It is a tool that helps the MPS to discharge its operational responsibilities, primarily to help it prevent and detect crime.

Key point for Authorising Officers: When considering the Deployment of LFR, each use is to be underpinned by an intelligence case to highlight the need to combat the relevant crime issue. Having identified a need, this will then allow Authorising Officers to consider the use of LFR. Authorising Officers need to decide the use of LFR is *necessary* and not just desirable to enable the MPS achieve its legitimate aim. In deciding if the use of LFR is necessary, consideration should also be given to whether there is an alternative, including the viability and intrusiveness of any alternative.

Authorising Officers need to keep a record why they considered the use of LFR to be necessary, the issue the Deployment of LFR was intended to address and how LFR would be deployed to address that problem.

The following are examples of why LFR may be used as a necessary tool to assist the MPS in preventing crime and disorder. The examples are illustrative only and there will be other scenarios where the use of LFR is justified.

Terrorism example: The use of LFR will assist the MPS in fighting terrorism. By way of example, LFR could be deployed at international borders. Given the high number of people passing through travel borders each day, LFR can act as a valuable tool to assist police officers to identify those of interest to the police for terrorism reasons including those who may be travelling on false documentation. LFR has the ability to have a Watchlist that can be scoped to those who pose a travel risk. LFR therefore supports officers who have the challenge of being familiar with a potentially significant and rapidly changing number of persons who are often motivated not to be identified and where the consequences of a missed identification opportunity can be catastrophic. Using LFR in this way would help the MPS achieve its aim of preventing crime and disorder and protecting the public through the disruption of those seeking to commit terrorist offences by making it harder to travel undetected across borders.

Child sexual abuse and exploitation example: The use of LFR will assist the MPS in fighting child sexual abuse and exploitation. LFR could be deployed based on intelligence to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse and exploitation. Missing person investigations use significant police resources where the need to locate and make an identification is often time critical. In such circumstances, it is of great importance to use all reasonable measures, to have the best chance of making a successful identification when the often scarce identification opportunities arise. At times, the police may also enlist the public to help with identifying missing people through the use of public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use LFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers the MPS a route to discharge its common law responsibilities to protect life.

Additionally, in a climate where police forces need to operate efficiently, the MPS has also identified that technology such as LFR can assist with the challenges of quickly and cost efficiently locating those with outstanding warrants or who have otherwise breached their bail conditions. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances. The *Bridges* case supports that there is a "considerable additional benefit to the public interest to including those wanted on a warrant" for a Deployment of LFR, even when there is no specific intelligence to place them in the area of the Deployment. The intrusion to those passing the system is no greater, but (i) the potential to protect the public from those wanted by the courts, (ii) the results from Deployments where those with outstanding warrants were included and (iii) the resultant arrests justified the inclusion of those with outstanding warrants from the courts as a *necessary* action to bring offenders to justice.

3.8 <u>The use of LFR is *proportionate* to legitimate aim being sought</u>

When considering the Deployment of LFR, the benefits of using LFR for an investigation or operation should not be disproportionate or arbitrary. In this respect the Surveillance Camera Commissioner recognises that:

"used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".

In this respect, the following factors (amongst others, depending on the nature of the Deployment) will guide Authorising Officers:

(a) *The use of LFR should be a reasonable use of MPS powers - it will not be proportionate if the proposed use of LFR is excessive in the overall circumstances of the investigation or operation.*

Authorising Officers will need to consider the seriousness of the investigation and the potential benefits of using LFR and balance this with any wider impact its Deployment may have to those on a Watchlist and the public at large. This will allow a decision to be made as to whether LFR is appropriate for use. Authorising Officers must give consideration to the composition of the Watchlist compiled for the LFR system to match against, to ensure that it is not compiled in an excessive manner. The Watchlist needs to satisfy the necessity and

proportionality test and will therefore be bespoke for each Deployment of LFR to ensure it meets the aims of that Deployment.

An objective for the use of LFR is to identify individuals who are of interest to the MPS and to utilise LFR technology with a view to apprehending them, reducing the prevalence of crime within the relevant area. With this is mind, the Watchlist compiled for each Deployment of LFR should be based on those currently of interest to the MPS and/or wider UK law enforcement to mitigate the risk of the LFR system matching with those no longer of interest to the MPS and/or wider UK law enforcement.

(b) *Consideration should be gives as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference.*

The use of LFR should be considered against other methods of locating persons of interest to the MPS and/or UK Law Enforcement. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation or Deployment.

Example: Circulating a wanted image on social media may be considered as an alternative to the use of LFR.

The use of LFR can be targeted to a specific area and does not result in the public being made aware of the identity of a person being sought by the MPS. It can also be used for a limited period, targeted, based on wider intelligence, to times and places when it might be most expected to locate an individual.

By comparison, social media results in a person's image being put into the public domain in a less targeted way. Once online, the image is public and the MPS no longer has control of that image. It therefore has potential to remain online even when the person has been traced and thus is a greater intrusion into the privacy of the individual being sought.

The Authorising Officer considering the use of LFR should balance any intrusion into privacy against the need for the investigative activity. If the Authorising Officer uses LFR in a way which minimises any impact it may have on a person's privacy as far as possible, it may offer a more appropriate, less intrusive alternative to a social media

Key point for Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record what other methods, as appropriate, were either not implemented or have been employed but which were assessed to be insufficient or inappropriate to fulfil the MPS's aim.

(c) *How and why the methods adopted will cause the least possible inference to the person(s) sought and others must be addressed.*

All uses of LFR under this Legal Mandate will be overt. LFR will be used for a limited time, with a limited footprint, with a limited purpose of seeking to identify those whose presence is of justifiable interest to the MPS. The LFR system will be visibly deployed in an open and

transparent way. Consistent with the principle of engaging with the public, signage will also be used to make the public aware of LFR prior to them entering the LFR system's range.

Key point for Authorising Officers: When considering the use of LFR, Authorising Officers will need to assess and minimise any impact on those who pass the LFR system to manage and mitigate any collateral intrusion.

Controls are also designed in to the LFR system and its operation to help minimise any impact on the wider public as follows:

1. LFR cannot be used to identify persons unless they have been included on a Watchlist.
2. The creation of any Watchlist is specific to each Deployment of LFR; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching. Images on a Watchlist will be lawfully held by the MPS with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Watchlist.
3. On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate LFR Alerts.
4. The cameras used in the LFR system are of sufficient quality for the LFR system's needs.
5. The LFR system is 'closed' and not connected to other MPS systems or the internet.
6. The LFR system is designed to assist MPS personnel to make identifications. The LFR system will always flag potential matches to at least one member of MPS personnel for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.
7. LFR Deployments and the materials that support LFR Deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

Controls have also been implemented with regards to personal data retention to minimise the impact on the wider public and those on the Watchlist. 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 the 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 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.

Authorising Officers also should consider the reasonable expectations of privacy the general public as a whole may have when traversing a public place where LFR is being considered for Deployment, when establishing if the proposed use for LFR is proportionate. Some places by their nature attract greater privacy expectations than others. Authorising Officers need to consider what measures are appropriate to identify the use of LFR when it is deployed, particularly where expectations of privacy may be greater.

Example: The public's expectations of privacy will be different in different public spaces. In Central London, the public has historically been protected by initiatives such as the 'ring of steel'. The public is also accustomed to an extensive use of similar systems such as CCTV, police patrols and other crime fighting/public safety systems deployed in order to ensure public safety. By comparison there could be a higher expectation of privacy in a quiet outer London suburban street, albeit the public would still expect the police to conduct investigations to prevent and detect crime. The use of LFR may also be more expected in areas which have high rates of crime where police action would be more expected.

Areas assessed as having high expectations of privacy which give the public little option to avoid the LFR area without substantial inconvenience should generally be avoided unless the following mean that the Authorising Officer is satisfied the use of LFR in the circumstances remains necessary and proportionate:

1. the importance of using LFR in that location to realise a legitimate aim supports LFR's use;
2. the lack of a viable, less intrusive alternative available for use in the circumstances; *and*
3. any further mitigations to reduce any impact to the wider public.

Example: If there was a necessity and proportionality case, based on intelligence, to deploy LFR in a residential area to identify a group of violent robbery offenders, then we understand there may be a greater expectation of privacy in this area. To mitigate this, depending on the circumstances we may provide additional communication about the use of LFR, for example by leafleting local residents or posting on local neighbourhood social media groups.

Key point for Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record the measures taken to ensure the use of LFR causes the least possible interference to the person(s) sought and others. Authorising Officers should then continue to review Deployments of LFR to ensure the use case remains appropriate.

3.9 Wider Human Rights Act considerations

The right to privacy is a value which protects the autonomy and human dignity of individuals by enabling them to conduct their lives in a way of their choosing. There are therefore circumstances when freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and of association (Article 11) may be particularly relevant and the use of LFR in these circumstances will also need to be considered necessary and proportionate.

Example: The use of LFR can assist the MPS in policing an assembly or demonstration, particularly where there is an intelligence case which supports there being a risk to public safety. In these circumstances, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to identify them. In deciding the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of the LFR Deployment.
Article 10 and 11 rights therefore need to be weighed against the need to use LFR to enable an assembly which might otherwise be disrupted given the identified risk to public safety. In making this decision, consideration should be given to factors which could help minimise the impact on Article 10 and 11 rights. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety. They could also include there being a particular focus placed ensuring the public understand the use of LFR is to help them safety undertake their assembly or demonstration.

4 Equality Act 2010

4.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination based on different treatment on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, the MPS must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty.

4.2 The MPS is required to take measures to ensure that the use of LFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of the LFR system, and (b) the operational Deployment of the LFR system:

(a) *The technical performance of the LFR system.*

The MPS LFR Documents are responsive to the Subject, System and Environmental Factors to ensure the LFR system is suitable for its intended use. Subject, System and Environmental Factors including aspects such as camera configuration, camera location, lighting conditions, the distance at which people will pass the LFR system and points relating to an individual's age and appearance have been considered carefully in the MPS LFR Documents to ensure the efficacy of the LFR system and the MPS's compliance with its Equality Act 2010 duties.

By way of example, the MPS LFR Documents provide that LFR Operators are trained to identify Watchlist issues with proposed images which may impact on system performance. Where the need to use an image is deemed to be necessary and proportionate in, those using

the LFR system have received training to maximise the LFR system's performance and to effectively consider any issues arising from the use of such images as part of the identification process.

Additionally, recognising that performance can vary by algorithm and in light of points relating to Subject, System and Environmental Factors, the MPS has adopted an "important fail-safe" highlighted in the Bridges judgment. This provides that absent there being other lawful grounds to take policing action:

> **no Engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own opinion that there is a probable match between the member of the public and the Watchlist image.**

This means the LFR system is not making any decision to Engage with the public, the officer is making this decision - just as officers make similar decisions to Engage with members of the public every day (without the support of LFR). The officer is best placed to make this decision, drawing on their training and policing experience.

Similarly the officer is best placed to consider the impact of any Subject, System and Environmental Factors which may have influenced the LFR system when it generated an Alert and if such factors combine to mean an Engagement with a member of the public is not appropriate in the circumstances.

Key point for Authorising Officers: In order to ensure that the officer is best able to make an informed decision on any Engagement, all officers who are part of an LFR Deployment are to have been briefed on the operation of the LFR system. This includes Subject, System and Environmental Factors that can impact performance. LFR Engagement Officers should also have been given training relating to unconscious bias given their key role in the Engagement decision making process.

(b) *The operational Deployment of the LFR system.*

MPS personnel are familiar with managing this requirement from a number of other crime fighting techniques such as 'stop and search'. In this respect, it is important that the use of LFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment informs the policing plan to support the Deployment of LFR to mean the MPS upholds the Public Sector Equality Duty. Compliance with the Equality Impact Assessment should then be monitored and reviewed for the duration of that Deployment.

5 Data Protection Act 2018

5.1 The MPS processes personal data for LFR 'based on law'; specifically its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate.

5.2 For the purposes of preventing crime and disorder, Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including any special category data, whether processed on a computer, CCTV, still images or other media. Any recorded image from a device which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR both in terms of identifying those on a Watchlist but also in terms of processing biometric information of members of the public to confirm they are not on a Watchlist. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

"For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

Key point for Authorising Officers: Authorising Officers already need be satisfied of the necessity to use LFR to prevent crime and disorder in the context of the Human Rights Act 1998. Similarly, to satisfy Section 35(5) DPA, they need to be content that the LFR system's processing of biometric data is strictly necessary for the law enforcement purpose. The law enforcement purpose should be clearly identified.

(a) Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via LFR is not used in a manner that is contrary to the identified law enforcement purpose.

(b) The 'strictly necessary' standard may be informed by the Authorising Officer considering factors including:

(i) what other policing methods have been used / discounted when seeking to locate an individual(s) on the Watchlist or to provide a series of tailored security measures;

(ii) the importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose through the Deployment of LFR at a given location (for example, is the Deployment intelligence-led or otherwise supported by information which confirms that LFR can be expected to get results in the circumstances being contemplated);

(iii) the size and scale of the planned LFR Deployment and the level of special category processing anticipated as a result of the LFR Deployment; *and*

(iv) if the law enforcement purpose which underpins the use of LFR is strictly necessary and proportionate to the need to undertake special category data processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

Example: alternative policing methods to prevent threats to public security: LFR may be deployed to police a high profile well-attended public event. When considering alternatives, in this example, other measures such as extra CCTV may be considered. However they will not always be a viable less intrusive alternative in the circumstances. For example:

1. Whilst CCTV can help ensure event safety, it lacks the ability to actively Alert officers to the potential presence of individuals of interest to them.
2. It may not be practical to expect officers to recognise larger numbers of people of interest to the Police given the nature and scale of the event, the numbers of officers available to police the event and the flow rate and number of people passing the CCTV system. This is especially relevant where the importance of making such identifications supports the use of a more suitable alternative such as LFR.
3. Where LFR is thought to offer further important protection to the public as opposed to other policing methods. For example, this may apply where the law enforcement purposes for a Deployment include wider public safety considerations. These may include the need to locate those wanted by the courts. Such persons may attend such a high profile event and, in line with the decision of the courts to require their arrest, pose a risk to the public generally.

Key point for Authorising Officers: Authorising Officers need to be satisfied that the processing satisfies one of the Schedule 8 conditions set out below and complies with the six data protection principles.

5.3 Schedule 8 conditions of the DPA are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; *and*
- necessary for archiving, research or statistical purposes.

Example: The use of LFR will assist the MPS in fighting knife and gun crime in support of its common law policing powers. LFR could be deployed to identify wanted offenders who have failed to comply with court bail relating to such offences. Used in this way, LFR would assist in the prevention, investigation, detection or prosecution of criminal offences.

LFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description to scan a crowd and try and spot an offender where positive results would otherwise be less likely and the risk of people being missed, higher. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context LFR's use may be seen as strictly necessary to support the investigation of knife and gun crime, to enable the MPS to effectively respond to a pressing social need.

Similarly, the Schedule 8 condition of being necessary for judicial and statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe. For similar reasons, the court in the *Bridges* case accepted the substantial public interest in the police using LFR to discharge their common law policing duties.

5.4 The MPS has also undertaken a number of steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the LFR system. Particular actions are set out in the remainder of this section.

5.5 *Data Protection Impact Assessment:*

A DPIA has been conducted to support the use of LFR in order to identify and minimise the data protection risks. Whilst the overall DPIA will be reviewed annually, Authorising Officers authorising the use of LFR should ensure there is a DPIA in place which is sufficient for each Deployment. Specifically, consideration should to be given to:

(a) if the risks and controls remain current and sufficient for the planned use of LFR; and
(b) if the planned use for LFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.

5.6 *Data Protection by Design*:

A number of data protection controls have been designed into the LFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into LFR processing activities. The designed-in measures identified at paragraph 3.8(c) of this document, include measures to:
(a) limit the amount of personal data collected;
(b) limit the extent of personal data processing;
(c) limit the period of personal data storage.

Additionally consideration has been given to limiting access to any personal data retained for the 31 day period. The LFR system also includes a number of physical and technical security measures including:

(a) Images are transferred onto the LFR system via a USB using an AES-CBC 256-bit full disk hardware encryption engine, that is further protected by pass-number access;
(b) 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;
(c) Role based access controls with limited user permissions are implemented on the LFR system;
(d) The LFR application is connected to mobile devices using a private access point with three levels of protection (i) specific IP addressing, (ii) password access to the access point, and (iii) password access to the mobile app. The mobile app has a RESTful API and will be covered by SSL;
(e) The Dashboard and RESTful API are secured with SSL and TLS by default;
(f) All connections are directed through HTTPS ;
(g) A full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*
(h) Technical issues with the LFR system are always dealt with by member of the technical staff who support the Deployment of the LFR system.

5.7 *Appropriate Policy Document:*

Section 42 of the DPA requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. This document includes details of:

(a) Procedures and safeguards for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
(b) the MPS policy for the retention and erasure of personal data for LFR processing.

5.8 *Data Protection Officer:*

The MPS has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to LFR. The DPO is available to inform and advise the Commissioner (as data controller) and MPS personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

6 Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a new surveillance camera code issues by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. Section 33(1) PoFA requires the MPS to have regard to the Code for the use of LFR. This includes compliance with the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which the MPS have regard to as follows:

Code	MPS approach
Fair processing information to data subjects	The MPS processing information publically available to data subjects. It makes information relating to the LFR and data processing available via its website. The LFR Deployments are publically disclosed with supporting information.
Appropriate retention and disposal systems	The necessary systems are addressed in the MPS LFR Documents.
Suitable technological and physical security measures	These measures have been addressed by design and are also covered in the MPS LFR Documents.
Cameras of sufficient quality to meet the intended purpose	This requirement is addressed by the design of the LFR system.
Monitored by trained individuals	The LFR system will always flag potential matches to a trained member of MPS personnel for a decision on any further action. In this way, the LFR system works to assist MPS personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.
Some level of human interaction	

The MPS has also given regard to the Surveillance Camera Commissioner's guidance on the use of automated facial recognition technology with surveillance camera systems in order to comply with Code and its obligations under s.33 PoFA with a number of points being covered in this Legal Mandate.

7 Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

(a) public authorities are obliged to publish certain information about their activities;
(b) members of the public are entitled to request information from public authorities.

In recognition of its FOIA duties, the MPS makes significant LFR information available via its website. This includes summary information relating to LFR Deployments including the Watchlist size, the total number of Alerts, positive action and incorrect identification numbers, arrests and disposal numbers and estimates of the total number of faces seen as people passed the LFR system. The MPS will also be responsive to FOIA requests.