Protective marking:	Official
Publication scheme Y/N:	No
Title:	Standard Operating Procedure for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology
Version:	Version 1.0
Summary:	Establishes procedures for the Deployment of Live Facial Recognition (LFR) technology in support of policing operations.
Branch/ OCU:	MPS LFR
Review date:	24/01/2021

STANDARD OPERATING PROCEDURE (SOP) FOR THE OVERT DEPLOYMENT OF LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY

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

1 Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool.

2 Application

2.1 All Metropolitan Police Service (MPS) police officers and police staff, including the extended police family and those working voluntarily or under contract to the Mayor's Office for Policing And Crime (MOPAC) or the Commissioner must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.

2.2 This SOP applies in particular to officers and staff in the following roles:-

a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the planning and Deployment of LFR technology; *and*

b) All police officers and police staff involved in any subsequent investigation resulting from the operational Deployment of LFR technology; *and*

c) All Authorising Officers (AO); *and*

d) The operational command team for any LFR Deployment (Gold, Silver and Bronzes); *and*

e) LFR Operators and LFR System Engineers.

Note: This list is not intended to be exhaustive.

3 Terminology

3.1 This SOP focuses exclusively on LFR**.** Terminology relating to LFR is defined in the MPS LFR Guidance Document.

4 Authority to Deploy LFR

4.1 In normal circumstances the authority given by an AO to Deploy LFR in support of a policing operation should be made by an officer not below the rank of Superintendent. Their authorisation should be recorded in writing.

4.2 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an MPS officer of NPCC rank[1] must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-London issues are taken into account as much as possible. This affords NPCC the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

4.3 Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable.

4.4 The authority of the AO:-

a) must articulate the legitimate aim of the Deployment and the legal powers that are being relied upon to support the Deployment; *and*

b) means that the AO is satisfied that the Deployment complies with MPS LFR Documents, or is otherwise authorised; *and*

c) must, from a Human Rights Act 1998 perspective, articulate (i) *how* and *why* the Deployment is necessary (*and not just desirable*), and (ii) is proportionate to achieve the legitimate aim of the Deployment; *and*

[1] NPCC –`NPCC rank' denotes an officer holding the rank of Commander or above.

d) must, from a Data Protection Act 2018 perspective, articulate that it is **strictly** necessary for the MPS's law enforcement purposes; meaning there is a `pressing social need' and it is not reasonably viable to address this through less intrusive means, either because less intrusive tactics have been tried, or it is reasonably believed that those tactics are unlikely to be effective; *and*

   i. Necessary on at least one of the following grounds (the ground(s) to be confirmed by AO):-

      a. Necessary for the MPS's lawful policing purposes[2] for reasons of substantial public interest; and / *or*
      b. Necessary for the administration of justice; and / *or*
      c. Necessary for the safeguarding of children and/or of individuals at risk; *and*

   ii. Necessary notwithstanding any expectations people may have pursuant to their Article 8 human rights regarding the respect of private and family life, as well as other human rights considered by the AO; *and*

e) must articulate that the AO has given regard to the safeguards proposed for the Deployment and the safeguards contained within the MPS LFR Documents, and considers that the Deployment in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the Data Protection Act 2018; *and*

f) means that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the Watchlist complies with MPS LFR Documents, including the legality, necessity and proportionality criteria; *and*

g) must articulate any authority to include additional categories of persons to the Watchlist, including the legality, necessity and proportionality criteria, in addition to those included to meet the primary purpose of the Deployment; *and*

h) means that the AO is directing that all police officers / staff engaged in the Deployment must have received MPS LFR training as per the MPS LFR Documents; *and*

i) means that the AO considers that the Deployment is proportionate with the benefits anticipated from the use of LFR outweighing the concerns and

[2] This being defined as "is necessary for the exercise of a function conferred on a person by an enactment or rule of law" in the Data Protection Act 2018. This will typically be the ground relied on to support MPS Deployments of LFR since this recognises the policing powers conferred on a Constable.

impacts there may be in relation to people's human rights and rights relating to equalities; *and*

j) means that the AO is satisfied that the control measures in the Data Protection Impact Assessment, Community Impact Assessment, and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the Deployment.

4.5 In cases of urgency an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency. All authorisations must comply with the requirements set out in paragraph 4.3.

4.6 Situations where the need for an authorisation to be granted urgently would include:-

a) an imminent threat-to-life or of serious harm to people or property; *and / or*

b) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which supports the urgency of action.

4.7 If an authorisation is given under the urgency criteria above, it shall be the duty of the AO who gives it, to inform an officer of the rank of Superintendent or above as soon as practicable, that LFR has been deployed and the reasons why. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

4.8 Should a further law enforcement purpose be identified after the AO has issued their authority for an LFR Deployment, processing in respect of the law enforcement purpose is not permissible unless the AO grants a further authority for it. 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.

5 Date, Time, Duration and Location of Deployment

5.1 The AO should define the date, time, location and duration the Deployment is authorised for.

5.2 During any policing operation where LFR is Deployed, signs publicising the use of the technology must be prominently placed in advance (outside) of the Zone of Recognition. This is to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition.

5.3 If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of a policing power. MPS staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.

5.4 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. Any person who requires further information relating to LFR should be provided with contact information for the MPS LFR operational team (LFR@met.police.uk).

6 Watchlist Generation

6.1 This section covers the generation and management of Watchlists to be used in LFR Deployments. Watchlists for use with LFR must be specific to an operation or to a defined policing objective. Watchlists:-

a) must be reviewed before each Deployment to ensure that all images meet the necessity and proportionality criteria for inclusion, and the make-up of the Watchlist should not be excessive for the purpose of the LFR Deployment; *and*

b) must only contain images lawfully held by the MPS; *and*

c) must only use images where all reasonable steps have been taken to ensure that the image is of a person intended for inclusion on a given Watchlist; *and*

d) 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.

6.2 Each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be aged under (i) 18-years-old and (ii) under 13-years-old.

6.3 Given the potential for System Factors relating to age, specific regard needs to be had to the importance of locating those aged under-18 on a risk-based approach in line with the MPS Documents, with a particular focus on ensuring the necessity case is fully made out.

6.4 If LFR is to be used to locate person aged under 13-years-old, specific regard should be had to anticipate LFR system performance issues. Specific advice must (at this time) be sought from the Directorate of Legal Services and the MPS LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO.

6.5 Examples of images that may be deemed appropriate for inclusion within an LFR Watchlist include:-

a) custody images of individuals:-

i. wanted by the courts; *and / or*

ii. wanted for arrest by, or are otherwise of interest to[3], the police; *and / or*

iii. subject of a court order, bail conditions, or other restriction that would be breached if they were at the location at the time of the Deployment; *and / or*

iv. missing persons deemed to be vulnerable / at risk; *and/or*

v. presenting a risk of harm to themselves or others.

b) police originated non-custody images involving (requires case-by-case assessment):-

i. wanted by the courts; *and / or*

ii. individuals wanted by, or who are otherwise of interest to, the police; *and / or*

iii. subject of a court order, bail conditions, or other restriction that would be breached if they were at the location at the time of the Deployment; *and / or*

iv. missing persons deemed to be vulnerable / at risk; *and / or*

v. individuals presenting a risk of harm to themselves or others (requires AO authority).

6.6 Non-police originated images must not be considered for inclusion in a Watchlist without formal authority of the AO.

Additional Watchlist Categories

6.7 It may also be appropriate to include Additional Watchlist Categories into a Watchlist, in addition to those included in a Watchlist to meet the primary purpose of the Deployment. These Additional Watchlist Categories are further considered as follows:-

a) Those with outstanding arrest warrants or are otherwise required by the courts within the MPS area.

The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general. In such circumstances, and noting that this is limited to those wanted by the courts within the MPS's area of operation, it is appropriate to consider whether LFR should be used to locate these people.

[3] `Otherwise of interest to'; Includes individuals who do not fit other criteria, e.g. a close associate (partner etc.) of someone who is particularly dangerous and wanted for a particularly serious offence (e.g. murder). The threshold for inclusion remains just as high, and in the example provided, the applicant would need to able to demonstrate how inclusion of the individual will help locate the person who is wanted. The applicant would have to demonstrate necessity and proportionality for inclusion.

b) *Those identified as suitable for inclusion on an LFR Watchlist where the purpose of locating these individuals is compliable with the Deployment's legitimate aim for the Deployment and compliments the Primary Watchlist Category.*

In a situation where the need to use LFR to locate those included on the Primary Watchlist Category has been established, there may be circumstances where it is also justified to use the same Deployment to locate persons beyond those included in the Primary Watchlist Category. In these circumstances, the intrusion to the public passing the LFR system is no greater, with the need to Deploy having already been made out. There may however be an opportunity for LFR to further protect the public by locating other people wanted by the MPS, people who are missing or otherwise vulnerable and at risk, and those who are consider high risk individuals.

The use of Additional Watchlist Categories can assist in these circumstances, providing the need to locate each individual passes the necessity threshold, and is proportionate in the circumstances. The use of Additional Watchlist Categories must also be in furtherance of the Deployment's legitimate aim, and the considerations relating to the composition of the Watchlist outlined in the remainder of this section apply equally to Additional Watchlist Categories. This is not least as the addition of any image to a Watchlist involves the processing of that person's data and is an interference with their Article 8 Rights. For these reasons, the decision to include any Additional Watchlist Category needs to be fully articulated in the LFR Application and authorised by the AO.

c) *Those identified by investigating officers as suitable for inclusion on an LFR Watchlist. This includes:-*

   i. *individuals in breach of bail conditions; and*

   ii. *missing persons who are considered vulnerable / at risk; and*

   iii. *individuals presenting a risk of harm to themselves or others.*

In these circumstances, the investigating officer (IO) is best placed to assess the need to locate an individual and why LFR is both necessary and proportionate in the circumstances. The IO will also understand what efforts have been made to locate the person, or why other options may not be viable in the circumstances. Where an IO decides to pursue use of LFR, they should record their decision and rationale in writing using systems such as CRIS, Crimint, and Merlin. The IO must contact the LFR operational team to have individuals added to the Watchlist, and ensure that they keep their decision to pursue the use of LFR under review. **When an individual no longer needs to be on a Watchlist, the IO must contact the LFR team to have the individual removed with immediate effect**.

6.8 When the AO considers authorising the inclusion of Additional Watchlist Categories, the AO must have regard to the nature of the Deployment when considering

Watchlist composition so as to ensure it is not excessive. Factors that may favour the inclusion of Additional Watchlist Categories include:-

d) the LFR Deployment is in area where there is a high flow of people; *and*

e) the LFR Deployment is in an area frequented by the transitory public; *and*

f) the LFR Deployment is to take place in areas where intelligence, other information and / or the AO's experience mean that it is reasonable to suspect that those wanted might be located with the help of the Deployment; *and*

g) potentially increased public safety gained from the inclusion of Additional Watchlist Categories.

7 MPS LFR Documents

7.1 **Assessments**; For each authorised LFR operation, the following assessments need to be created, reviewed, and amended where necessary:-

(i) Data Protection Impact Assessment* (Review/Amend/Adopt); *and*
(ii) Equality Impact Assessment* (Review/Amend/Adopt); *and*
(iii) Community Impact Assessment* (Review/Amend/Adopt); *and*
(iv) The Surveillance Camera Commissioner's Self-Assessment* (Review/Amend/Adopt); *and*
(v) LFR Risk Assessment (carry out).

Note: *Any assessment listed above showing `Review/Amend/Adopt' has already been created by the MPS LFR team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each LFR operation.

8 Risk Assessment & Resource Levels

8.1 Each Deployment should be risk assessed and the appropriate risk assessment documents completed. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.

8.2 The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.

8.3 Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond

effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.

8.4 LFR System Engineers will be deployed to support LFR Deployments and will come with suitable vehicles where required.

8.5 All MPS officers and staff deployed on LFR Deployments must be compliant and in-date with MPS emergency life support (ELS) and officer safety (OST) training requirements. Exceptions to this must be specifically addressed within the written risk assessment. All MPS officers and staff involved in an LFR Deployment must receive LFR training prior to being deployment.

9 Planning & Booking

9.1 As part of the LFR planning process and before the AO authorises a Deployment, the MPS LFR team (including LFR System Engineers) should be consulted on the appropriateness and viability of a Deployment.

10 LFR Operational Roles

LFR Command Team

10.1 LFR Deployments must be supported with a clear command structure. The following roles are defined for the purpose of creating an appropriate hierarchical command structure:-

a) Gold Commander (Superintendent or above[4]); There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their `strategic intention' aligns with the Written Authority Document. Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold will also liaise as necessary with NPCC ranked officers. Gold can also perform the AO role.

b) Silver Commander (Inspector or above); There is only one Silver Commander for any LFR Deployment. Silver reports to Gold. Silver has tactical command of the Deployment and is responsible for tactical implementation. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having particular

[4] Note that where the urgency criteria (para 4.4) has been applied, the Gold Commander may be of Inspecting rank. However, this should revert to Superintendent or above as soon as a Superintendent reviews the Deployment and provides authority for the Deployment to continue.

regard to the effectiveness of the safeguards in place whilst LFR is being used.

c) Bronze Commander (Sergeant or above); Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with sufficient clarity, and ensure that they are fully understood by all officers and staff involved in the Deployment.

d) Bronze Community; Bronze Community is an individual appointed by Silver specifically to oversee and manage community / stakeholder engagement relevant to the LFR Deployment.

10.2 Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative command team terminology, or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

LFR Operator

10.3 LFR Operators receive detailed training prior to being deployed operationally. Their role is to monitor and assess system Alerts, before working with LFR Engagement Officers (as necessary) to decide whether an Engagement is required.

10.4 The LFR Operator should log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR system performance to the Silver Commander.

10.5 The LFR Operator's log should include:-

a) the LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; *and*

b) what decision was taken regarding whether to Engage a member of the public or not; *and*

c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

LFR Engagement Officer

10.6 LFR Engagement Officers must have an understanding of the LFR system, how it performs, and what effect Subject, System, and Environmental Factors might have.

These officers must receive a full operational briefing prior to deployment. These officers may be deployed in uniform or plain clothes.

10.7 When conducting an Engagement, LFR Engagement Officers must ensure that they do so lawfully, and in an appropriate and proportionate manner. Officers must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject of an Engagement, should be supplied with an LFR information leaflet.

10.8 The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place[5]. The LFR Engagement Officer should receive an Alert on their handheld device (or otherwise had sight of it) and must then make their own decision about whether they should instigate the Engagement or not. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.

10.9 When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal.

10.10 Whilst officers must exercise their own discretion when using their powers of arrest and detention, MPS policy is that an LFR system-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

10.11 If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

10.12 After any Engagement (that follows an Alert), the LFR Engagement Officer must update the LFR Operator with the outcome of that Engagement.

10.13 Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no

[5] The driving force behind this point is that an LFR Operator should not be making the decision that an Engagement Officer carries out an Engagement. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own `reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take.

legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so.

LFR System Engineers

10.14 LFR System Engineers have enhanced technical training for the Deployment of LFR (see MPS LFR Guidance Document for further information). LFR System Engineers are responsible for the set-up of the LFR equipment and the optimisation of the LFR system to maximise performance.

11 Post-Deployment

11.1 Following each LFR Deployment, the Gold Commander must ensure that a post-Deployment evaluation is completed. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both *qualitative* and *quantitative* in nature.

11.2 The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the Deployment and what opportunities exist to improve them for future use, and how learning will be shared.

11.3 The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (<u>including</u> what methods were used to obtain them):-

a) total number of individuals ***<u>and</u>*** the total number of images included in the Watchlist (*there may be multiple images of some individuals*); *and*

b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR system was able to generate a Template from them); *and*

c) total number of LFR system-generated Alerts; *and*

d) total number of Alerts that do not result in an Engagement; *and*

e) total number of Alerts where a decision was taken to Engage an individual; *and*

f) total number of Alerts that are confirmed as correct (the individual is who the LFR system suggests are); *and*

g) total number of <u>correct</u> Alerts that result in an Engagement that do not require any further police action; *and*

h) outcome of each case where police action is instigated following an Alert; *and*

i) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome.

12 LFR System Security

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

a) images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine, that is further protected by pass number access; *and*

b) the LFR system is a fully-closed system with two layers of password protection to access the application; *and*

c) the LFR system is physically protected when in use and securely wiped following each Deployment; *and*

d) role based access controls with limited user permissions are implemented on the LFR system; *and*

e) 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*

f) the Dashboard and RESTful API are secured with SSL and TLS by default; *and*

g) all connections are directed through HTTPS; *and*

h) a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*

i) technical issues with the LFR system are always dealt with by LFR System Engineers deployed on the operation.

13 Data Retention & Data Management

13.1 The MPS must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the MPS LFR Documents. This means that:-

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

b) 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.

13.2 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:-

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

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

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

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

b) in accordance with the MPS's complaints / conduct investigation policies.

13.4 To support compliance the LFR system has a full audit capability, and the LFR Operator's log is retained in accordance with MOPI.

13.5 The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether or not protected by encryption, must be reported immediately to the AO, Gold, and the MPS Data Protection Officer.

Register of Deployments

13.6 Any Deployment of LFR must be recorded on a centrally held register. This register will record a number of things including:-

a) name and rank of the AO and command team; and

b) date, time, duration, and locality of Deployment; and

c) Watchlist composition statistics (not including any personal data); and

d) the number of Alerts and the various statistics relating to these; and

e) number of Engagements and their results;

13.7 The MPS will make information relating to LFR Deployments available to the public in accordance with the MPS LFR Documents.

14 Contact Information

14.1 The MPS LFR team can be contacted using the following email address; LFR@met.police.uk.

15 Further Documentation

15.1 Further documentation is available providing useful information relevant to LFR. This is detailed below.

a) Information Management APP; www.app.college.police.uk/app-content/information-management;

b) National Decision Model; www.app.college.police.uk/app-content/national-decision-model;

c) National Intelligence Management; www.app.college.police.uk/app-content/intelligence-management;

d) College of Policing Code of Ethics; www.app.college.police.uk/code-of-ethics;

e) Home Office Biometric Strategy – Published June 2018; www.gov.uk/government/publications/home-office-biometrics-strategy;

f) High Court Ruling – *R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin)*; www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.