	Publication (Y/N): Y
Title:	Metropolitan Police Service Privacy Impact Assessment
Summary:	Data Protection Impact Assessment for the use of Live Facial recognition within the MPS
Branch / OCU:	SCO35
Date created: 25.07.18	**Review date:** 25.07.19
Author:	DI Nigel Nelson

Contents

1. Introduction

In 2016, the MPS decided to trial the use of Live Facial Recognition, (LFR) in fixed plot environments with a view to evaluating it as an overt means of tracing wanted persons and enhancing safety at public events. A total of 10 events representing different physical and policing environments were chosen in order to assess under what conditions LFR could be most efficiently deployed. It has already been deployed at NHC 2016 and 2017 and the Remembrance day celebration on 12th November 2017, with further trials being scheduled to take place at sporting events, at transport hubs and other public events.

The use of LFR by the police will always be accompanied by human intervention, thereby ensuring that executive action will always be a consequence of an initial technological indication, sourced through LFR intervention being confirmed by intelligence enquiries undertaken at the time. LFR technologies only collect and store data under circumstances when image data collected results in the generation of alerts, which is then associated with image data retained on a watch list. All other data collected is discarded once it has been compared with that on the watch list.

LFR is intended to be utilised in the following applications:

- **To identify individuals shown as wanted by the police and the courts.**

The MPS are seeking to deploy LFR in order to identify individuals who are shown as wanted by the police and criminal justice systems. The utilisation of LFR will assist in the identification of offenders, thereby expediting their passage through the criminal justice system and therefore reducing the probability of repeat offending. The application of this technology will provide a more efficient and less intrusive means to identify and arrest wanted individuals in public spaces.

- **To identify individuals who present a risk of harm to themselves and others.**

LFR can provide event Commanders with an additional tactical option to enhance police capability within an operational policing footprint. This can be used to address a traditional crime issue, or reduce the risk of physical harm or violence through an intelligence based watch-list. This itself is focused on wanted individuals or identified individuals who may be drawn to an event who may cause safety implications for an event or themselves.

- **To support ongoing policing activity with regards to a specific problem or location.**

LFR can provide an additional asset to enhance a police response to address a particular issue, such as an increase of a specific crime type within a particular area. This will consist of a bespoke watch-list of wanted individuals or those with conditions not to attend an area based on intelligence and crime analysis.

- **To assist police in identifying individuals who may be at risk or vulnerable.**

LFR has the potential to be used to identify individuals who are believed to be vulnerable, missing, or suffering from mental health issues and at risk of harm.

LFR Methodology

Facial recognition biometrics relies on genetically determined physical features. When a facial image is captured, the raw data is normalized, (aligned to frontal pose) and irrelevant data such as the location, size of the face or frame is eliminated. The facial recognition algorithm extracts landmarks and generates a template from the relative position, size and shape of these features. Automated facial recognition technology was initially designed for subject compliant access systems and is dependant on a number of factors, including illumination, expression and the quality of the reference and captured images. The aim of trialling LFR in different environments and scenarios will generate an evaluation of the accuracy of LFR and identify its potential as a policing tactic.

LFR consists of a closed system of between 2 and 8 cameras directly connected to an integrated server and client monitor, secure access point and tablets or similar mobile devices. LFR does not integrate into existing CCTV infrastructure. Cameras should be situated to cover a pinch point location to capture the flow of people walking towards the camera. Facial images are detected, extracted and compared against the facial images on a watch list, which is bespoke and consists of images relevant to a particular deployment. Watch list images are sourced from the custody imaging system.

Where the system generates an alert against the watch list the extracted facial image and watch list image are displayed on the monitor and sent over the closed access point to password protected hand held devices.

Alerts are saved within the system, whilst facial images that do not generate an alert against the watch list are discarded. A report of all matches is saved from the LFR for auditing purposes. Current MPS retention, removal and disposal policies for material held will result in material used in a successful conviction being retained for longer periods of time.

How LFR works

A bespoke watch list is created for every deployment taking geography, the event and background intelligence into account. Images, usually taken from the custody imaging database or from images provided from specific sources of intelligence, for example from persons reporting vulnerable missing persons, will be uploaded on to the LFR watch list data base.

- All deployments will be in public spaces and will be overt and may be signposted, a consideration which will be decided upon by the Command team, who will take account of the aims and objectives of the operation. This will be in accordance with MPS signs with clear statements; ***Police Operation - Cameras in Use***. It will be further supported by leaflets which will provide information on the operation and a link inviting members of the public to share their views and complete a survey as part of the consultation process.

- Once police officers are in receipt of an alert, an assessment will be made of the images and associated information and, if necessary, the individual will be located and stopped and their identity confirmed.

- Faces detected by LFR which do not result in an alert will be automatically discarded. Images of matched 'alert' faces are retained for 30 days. The Data Controller believes this is necessary to justify police intrusion into individuals' lives and may become relevant if complaints or FOI applications are received after a stop generated by LFR. There is no retrospective searching or sharing of information.

2. Privacy Impact Screening Questions

		Yes	No
Q.1	Will the project involve the collection of new information about individuals?	X	
Q.2	Will the project compel individuals to provide information about themselves?		X
Q.3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	X	
Q.4	Will the MPS be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	X	
Q.5	Does the project involve the MPS using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	X	
Q.6	Will the project result in the MPS making decisions or taking action against individuals in ways that can have a significant impact on them?	X	
Q.7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	X	
Q.8	Will the project require the MPS to contact individuals in ways that they may find intrusive?		X

If the answer to any of the above questions results in a 'yes' then a DPIA is required.

3. European Commission of Human Rights considerations

European Convention of Human Rights:

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. 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.

The MPS is a public authority, therefore, is subject to a statutory duty under HRA Article 6(1) not to act inconsistently with a Convention right. The relevant Convention right for the purposes of this processing is Article 8(1) of the Convention.

It is the view of the MPS that Article 8(1) provides limited protection to the criminal and it is not intended to bar lawful and proportionate law enforcement activities. It is for this reason that the MPS believes that the interference with the Article 8(1) rights can be justified under Article 8(2). The purpose is the prevention & detection of crime, protection of the public and safeguarding vulnerable individuals. This falls squarely within one of the permissible bases for interference in Article 8(2), which refers specifically to the prevention of disorder or crime. However, the MPS recognises that for the interference to be justified it would need to be "*in accordance with the law*" and "*necessary in a democratic society*", within the meaning of Article 8(2).

4. Data Protection and 'Privacy Law' Assessment

1.	Does this project / initiative address a Pressing Social Need? If so, outline it here:

Protection of the public from crime and disorder, maintaining public safety and safeguarding vulnerable individuals is paramount to the MPS. This trial seeks to:-

- Arrest individuals wanted by the criminal justice systems.
- Provide a means of enhancing safety at public events through identifying those who pose risk through intelligence.
- Reduce risk of safety to the public through the identification of those posing such risk.
- Identifying vulnerable individuals.

This technology will provide police with the ability to identify individuals who are wanted by the criminal justice system or otherwise pose a risk to either themselves or the general public.

2.	Are your actions a proportionate response to the social need?

The headline privacy design features for this project are as follows:

- Individual's facial images are retained for the following times:

  (a) Images which are not positively identified against the watch list are discarded immediately after comparison has taken place.
  (b) Images which are identified against the watch list, however no further action is taken against the individual are retained for 30 days, should ROA applications be made under DPA 2018.
  (c) Images resulting in the individual being subject to criminal justice system prosecutions will have their images retained in accordance with MPS retention, removal and destruction policies[1].

- Operations take place in a public place and are not 'intrusive' or 'covert' as defined under RIPA 2000.
- This operation is a trial to assess the reliability and effectiveness of LFR technology & methodology for a proportionate and necessary policing purpose.
- All staff employed in the consequence of LFR operations will be security vetted MPS employees.
- Appropriate technical and organisational measures will be in place to safeguard against unauthorised loss, disclose or destruction of data used for the operation (uploaded facial images) or retained as a result of the operation (recorded positive matches)
- LFR generates alerts in respect of those whose facial images are identified on the watch list. Human intervention, based on intelligence database checks will always be undertaken before any executive action is taken.
- All LFR operations will be authorised by Commander Balhatchet, SCO35.
- Records will be retained in respect of all LFR requests, by reference to governance, command structure, relevance and operational objectives.

[1] Records Management - Retention Review and Disposal (RRD) Tables.pdf

5. Common Law, Duty of confidence

Common Law Duty of Confidence:

A breach of confidence will become actionable if:

- the information has the necessary quality of confidence;
- the information was given in circumstances under an obligation of confidence; and
- 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. If a person has provided consent for the processing of their information.
2. If there is a legal requirement to process the information.
3. If it is in the public interest to process the information.

It is in the public interest to process the information in order to:

- Arrest individuals wanted by the criminal justice systems, thereby enhancing public safety.
- Provide a means of enhancing safety at public events through identifying those who pose an intelligence based risk of harm at an event.
- Reduce risk of safety to the public through the identification of those posing such risk.
- Identifying with a view to ensuring the safety of vulnerable individuals.

6. Data Protection act 2018

Data Protection Act 2018

Principle 1, (Section 35 DPA 2018).
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

The processing of personal data for any of the law enforcement purposes 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 necessary for the performance of a task carried out for

1) that purpose by a competent authority.

sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and
(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—
(a) the processing is strictly necessary for the law enforcement purpose,
(b) the processing meets at least one of the conditions in Schedule 8, and
(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

Sensitive processing covers, “the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual”.

It must be stressed that there is no intention of the MPS to provide wide access to this data corporately. Nor indeed is it our intention to process this data beyond our core policing purposes.

For the avoidance of any doubt, this project relies on the following definition of policing purpose as defined by the Code of Practice on the Management of Police Information published 14th November 2005 by the Secretary of State for the Home Department:

a) The protecting of life and property
b) Preserving order
c) Preventing the commission of offences
d) Bringing offenders to justice, and
e) Any duty or responsibility of the police arising from common or statue law.

The Code of Practice further states in paragraphs 4.1.1 – 4.3.1 that:

"...Chief Officers have a duty to obtain and manage information needed for police purposes... [and]*...information should be recorded where it is considered that it is necessary for a police purpose..."*

It is the view of the MPS that the requirement for this processing to be both fair and lawful is met through the Pressing Social Need outlined in this DPIA.

Data Protection Act 2018:

Where the processing, by its very nature, may not be considered as fair or lawful, the MPS relies on the following Sections of the Data Protection Act 2018 when processing this information:

Section 30 (1) The processing of personal data by competent authorities for 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, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction.

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; and
(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.

10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law. The legal framework and existing body of guidance in which the MPS relies is provided by the following:

- NPCC Authorised Professional Practice (APP)
- Management of MPS Intelligence Policy
- MPS Intelligence Strategy
- MPS Intelligence Manual
- NPCC (2005) Guidance on NIM, NIM Codes of Practice & NIM Minimum Standard
- The Data Protection Act 2018

- 2010 Guidance on the Management of Police Information
- The MPS Data Protection Standard Operating Procedures (including international data processing compliance standards)
- The APP Data Protection Manual of Guidance
- MPS Information Governance Framework
- MPS Information Management Strategy
- MPS Information Management Policy
- MPS Security Code
- MPS Records Management Manual (including the Review, Retention and Disposal Schedule).

1.	How will you tell individuals about the use of their personal data?
The MPS has a mature Information Governance Strategy and Structure which requires the MPS to be open and transparent around the nature in which (sensitive) personal data are to be processed. The MPS has a Fair Processing Notice (FPN) provided at all Custody Suites and on the MPS internet site, which includes full details as to how a subject may exercise their ECHRA Principle 6 rights. The command team will identify other means of communicating with individuals through the distribution of leaflets and through the use of large CCTV screens.	
2.	Do you need to amend your privacy notices?
No, the existing Fair Processing Notice adequately covers the intended processing.	
3.	If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
No: Consent can be withdrawn by the data subject at anytime, thus requiring the MPS to delete the data and limiting the scope in which the MPS can fulfil policing purposes. Obtaining consent would prejudice the purpose in which the data is collected in the first place.	

Principle 2, (Section 36 DPA 2018). The second data protection principle is that— (a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.	
	The intended processing is outlined in Principle 1, b), within the Fair Processing Notice and the notification with the Information Commissioner's Office: Registration No: Z4888193.
1.	**Have you identified potential new purposes as the scope of the project expands?**
	No.

Principle 3, (Section 37 DPA 2018)

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The MPS only processes data that is relevant to policing purposes.

(a) Images which are not positively identified against the watch list are discarded immediately after comparison has taken place.
(b) Images which are identified against the watch list, however no further action is taken against the individual are retained for 30 days, should FOIA applications be made under DPA 2018.
(c) Images resulting in the individual being subject to criminal justice system prosecutions will have their images retained in accordance with MPS retention, removal and destruction policies.

Technical systems ensure that data is accordingly retained, as described a) – c). Processing mechanisms will be reviewed annually by Nigel Nelson in order to ensure that the personal data held is commensurate with policing purposes.

1	**Is the quality of the information good enough for the purposes it is used?**

The quality of the information retained is dependable on a match being identified on the watch list. LFR technologies have been tested under variable operating conditions by both the manufacturer NEO Neoface and the MPS during a series of three trials.

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

All personal data used is essential for the project and future deployment. Personal data is required to provide an evidential base in respect of evaluating the conditions and environment under which LFR can be deployed as a policing tactic.

Principle 4, (Section 38 DPA 2018)
The fourth data protection principle is that— (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and (b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.
The MPS acknowledge the concerns relating to the data subject, to the organisation and additionally to third parties, if the data processed was inaccurate. The watch lists are constructed from relevant intelligence, associated with the strategic intention of a deployment and checked to ensure for accuracy within 2 days of a deployment. Likewise, the retention of images for 30 days is monitored from the technical perspective of the operation and records are retained to identify the days upon which date must be deleted and as to the fact that this has been actioned.

1	**How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?**
Sensitive data is obtained via human intervention once the LFR technology has matched a facial image with information held on the watch list database. The subject will themselves be providing personal data, which will be verified through information and police intelligence databases.	

Principle 5, (Section 39 DPA 2018)
The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

1	**What retention periods are suitable for the (Sensitive) personal data the MPS will be processing?**
No data is held in respect of images which are not linked with the information held on the watch lists. Data will be retained in line with the MPS Retention, Review and Deletion policy. Data obtained as a consequence of a watch list alert is retained for 30 days in order to: • To complete technical analysis of the deployment and address any irregularities encountered. • To respond to any ROA applications under DPA 2018 or public complaints arising from the deployment.	

2	**Are you procuring software that will allow the MPS to delete information in line with our retention periods?**
Yes - the LFR database has the capability to be wiped clear of all data after each deployment.	

Principle 6, (Section 40 DPA 2018)

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

The MPS provides details regarding how a Data Subject can exercise their Principle 6 Rights within the MPS Fair Processing Notice and MPS internet site.

The only images that are retained by the LFR system are alerts against the watch list. The Review, Retention and Disposal of this data is highlighted in Principle 5.

Personal data retained can be accessed through applications through Right of Access applications DPA 2018.

7. Section 64, DPA; Data protection impact assessment.

Required within the LFR DPIA at the processing of data is likely to result in a high risk to the rights and freedoms of individuals. This is an assessment of the impact of the envisaged processing operations on the protection of personal data.

Risk identified with reference to processing operations.	Mitigation/ Reduction of risk	
The data entered onto the watch list is not treated within the correct Government Protective Marking Scheme, (GPMS).	• All MPS staff/ officers are trained in respect of the GPMS. Officers compiling the watch lists will perform this task in a secure environment to which the public do not have access. • All watch lists are appropriately stored prior to the operation and are deleted immediately after, unless individuals are dealt with for criminal justice matters, under which MPS case paper retrieval, removal or disposal parameters apply.	Watch list compilation and security.
The watch list contains inaccurate data.	• Watch lists are compiled some time prior to deployment, are bespoke to the operation and are reviewed again no more than 2 days prior to the operation to ensure that it only contains relevant and actionable data. • The technical team also review the watch list to ensure that the correct formatting/ inputting procedures have been followed to minimise the rate of false system alerts.	
The watch list data is disclosed to third parties.	• Officers/ Staff compiling the watch lists are briefed in respect of watch list circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff.	
Watch list data is not being correctly managed in respect of DPA 2018 and GDPR	• Processed lawfully, fairly and transparently: Watch lists are bespoke to a given operation and are formulated to respond to the aims and objectives associated from a given operational demand. All intelligence on police databases is held securely and assessed in respect of reliability. Reliable and provenanced information will be used in the compilation of watch lists. Procedures are in place to review the construction of watch lists. • Collected only for specific legitimate purposes and adequate, relevant and limited to what is necessary. Each watch list is bespoke to a specific operation and encompasses intelligence which reduces the risk to the public at a given event/location. • Must be accurate and kept up to date. Watch lists are compiled prior to an event however are reviewed within 2 days of the intended deployment. Procedures are in place to ensure that this is in practice and records are kept to reflect upon this. • Stored only as long as is necessary. All data is stored within either the LFR or the MPS retention, removal and disposal policies for criminal justice material. Watch This is lists are destroyed as soon as a deployment has taken place, unless individuals are arrested or a false positive identification is made. • Ensure appropriate security, integrity and confidentiality. All watch list data is compiled in accordance with the GMPS and data is treated accordingly.	

Risk identified with reference to processing operations.	Mitigation/ Reduction of risk	
The LFR equipment is not functioning correctly.	• A technical expert, 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. • A"blue watch list" is completed using police staff images, (voluntarily supplied) and these individuals will walk past the LFR recording apparatus before, during and after the operation. Records are maintained in respect of positive identifications, which are recorded. When a member of staff, who is on the "blue watch list" is captured by the equipment, however the LFR system fails to generate an alert, this results in a "false negative indication". These "false negative indications" are used to monitor the performance of the LFR equipment. • All relevant information is logged for auditory purposes.	Operational deployment of LFR
False positive identifications may lead to an unwarranted intervention by the police adversely affecting the rights and freedom of that individual.	• All images that result in a watch list alert will additionally be reviewed by the individual operating the LFR equipment prior to information being passed to intervening police officers. This will ensure that the biometric match relates to the person whose details are held on the watch list.	
An incorrect person is stopped by police as consequence of a correct watch list indication.	• 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 receiving officer therefore has a precise image of the person sought, negating the possibility of an incorrect person stopped.	
An unlawful arrest is made	• Officers are briefed prior to each deployment and are informed that LFR is a process which is only deployable in conjunction with human intervention. Once a positive warning has been identified, officers will be tasked to intervene and use intelligence databases and interactions with the individual to confirm if they are the same person as that on the LFR watch list.	
Retention data times not complied with.	• The LFR technical team run regular audits to ensure that all data on the LFR watch lists are only held for the minimum period of time as stated.	

Risk identified with reference to processing operations.	Mitigation/ Reduction of risk	
An individual who has been stopped as a result of an LFR alert wants to complain and/ or submit a FOIA.	• The LFR system has processes in place which retain images of those stopped as a result of a positive indication for 30 days, which provides sufficient time for a complaint / ROA request to be received and the relevant LFR data to be further retained. • Information leaflets are given out to all those stopped and others who may have their facial images compared with those on the database. This information encourages stakeholder feedback and provides contact details. • The command team will give consideration to signposting an LFR via large CCTV screens and other suitable means, advising of the fact 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 and will accordingly report any feedback to operational leads.	Post LFR deployment
Watch list data is disclosed following an LFR operation.	• Procedures are in place to destroy data on LFR watch lists after the operation has taken place. Exceptions to this are: i) Where the LFR identifies an individual who is subsequently confirmed as being wanted by the police/ criminal justice system. In these circumstances data is subject to MPS criminal justice retention, removal and disposal policies associated with the relevant offence. ii) Where a false positive identification is made, resulting in an individual being stopped and human intervention confirming that the individual stopped by police was not identical to the data stored on the watch list. In these circumstances data will be retained for 30 days in the event that a FOIA / complaint against police should be made. • In all instances data is retained on secure systems and will not be subject to illegal disclosure. Records will be maintained under situation ii) to confirm that the data has been disposed of after 30 days.	
Misinformation within the public, impacting upon trust and confidence in respect of LFR	• Stakeholder engagement strategy has been developed and will address relevant interaction. • Press and Media strategies have been developed. • Risk management strategies have additionally been developed in respect of this parameter.	

8. Miscellaneous considerations

1.	Complaint Handling
Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection and Freedom of Information Officer.	
2.	**Freedom of Information Act 2000 (FoIA)**
The MPS demonstrates a commitment to openness and transparency regarding this processing, subject to any limitations posed by security or confidentiality requirements. The MPS is a public authority for the purposes of the FoIA 2000. Any information held by the MPS is accessible by the public on written request, subject to certain limited exemptions. In line with guidance from the ICO, the MPS will place this DPIA and other associated documents on the FoIA Publication Scheme, so the public can be aware of how the MPS process personal data. The only exception to this will be the following: • Legal Advice • Commercially Sensitive material • Personal Data Pertaining to the Consultation Participants • Information which would otherwise affect the operations of the MPS and is not in the public's interest to disclose. All public requests for information should be directed to the MPS Data Protection and Freedom of Information Officer.	

9. Consultation Results

A stakeholder engagement strategy has been developed in order to both identify key stakeholders and formulate an effective means of communicating and developing trust and confidence in LFR technology and its application as a police tactic.

Stakeholder engagement strategy has been developed and inter laced with Press and Media and Risk Management strategies.

10. Implementation of DPIA Outcomes and Responsibilities

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?

	Action to be taken	Date for completion of actions	Responsibility for action
1.	Review PIA to ensure it remains focused on the LFR trial	Completed.	DI Nigel Nelson, DSU Bernie Galopin, Andrew Walker, (MPS, DPA), Johanna Morley, (MPS Technical and Innovation), Commander Ivan Balhatchet, (MPS Strategic lead, LFR)
2.	Review LFR retention and access policy as absent from initial PIA	Completed with DPIA review.	DSU Bernie Galopin, DI Nigel Nelson, Johanna Morley
3.	Formation of Strategic Oversight Board	Completed.	Commander Ivan Balhatchet

11. Specific Considerations for each event

This will be amended for each deployment and make reference to the intelligence supporting the deployment..

The intelligence supporting this deployment is incorporated within the Intelligence case which is documented in the Operational Mandate.

The overt nature of this operation will be highlighted through pre-event Press and Media releases and through signage on the day which will be prominently placed on the approach to the LFR cameras however outside the capture zone.

This DPIA complies with the requirements of Sections 35 – 40 and 64 of the Data Protection Act 2018.

12. Conclusion

The Data protection impact assessment has identified a number of relevant risks associated with the watch list compilation and security, Operational deployment of LFR and Post LFR deployment phases.

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 document and as such will be subject to continuous review.

12. Data Privacy Impact Assessment Sign-off

1.	**Project Sponsor / NPCC Lead**
	Sign Below: Name: Position: Date:
2.	**Head of Information Law and Security**
	Sign Below: Nigel Shankster, on behalf of; Name: John Potts Date: 12 June 2018