Greater Manchester Police

Data Protection Impact Assessment

GMP Deployment of Live Facial Recognition

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of the envisaged processing operations on the protection of personal data.

It is a checklist against Information Governance compliance and is a risk management process that enables Greater Manchester Police to anticipate and address likely impacts of new initiatives, to provide assurance of confidentiality, integrity, availability, data subject rights, IT security and data quality issues related to the project.,

This assessment **should be completed at the project planning stage** of any major project involving the use of personal data or if you are making a significant change to an existing process.

Notes on completion:

Please answer all questions in Section 1. Should all questions be answered "No" there is no requirement to complete Section 2. In such instances, please send the completed assessment to Information Compliance and Records Management Unit (ICRMU) via email to**:** dataprotection@gmp.police.uk.

If any answer in Section 1 is "Yes" please continue to complete Section 2 and send the completed assessment to the ICRMU as above.

Any queries during completion should be directed to the ICRMU. It follows the process set out in our DPIA guidance and this document should be read along with the guidance.

Any changes to original assessment must be notified to the ICRMU as above. Once all changes are completed, the final completed assessment must also be emailed to the ICRMU as above.

The ICRMU will ensure the Data Protection Officer comments on this assessment before final sign off.

VERSION CONTROL FOR THIS DPIA

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)
V0.1	21/1/25	Initial draft	Insp Jon Middleton
V0.2	29/01/25	IG 1st Review -	Rachael Bigland - ICRMU
V0.3	08/05/25	IG 2nd Review	Rachael Bigland - ICRMU
V0.4	12/06/2025	IT and Project team review	Andrew Spillane
V0.4	26/06/2025	IG 3rd review	Steve Lewis - ICRMU
V0.5	05/08/2025	IT and Project team review	Paul Savill - IT
V0.6	08/09/2025	IT and Project team review	Michael Booth - Change
V0.7	12/09/2025	IG 4th review	Steve Lewis – Information Governance
V0.8	02/10/2025	DPO final review	Suzanne Martin
V1	16/10/2025	DPO sign off	Suzanne Martin

Overview

Project/System/ Initiative	GMP Deployment of Live Facial Recognition					
Information Asset Owner	IAO – Chief Supt. Neil Jones SPOC - Inspector Middleton					
Department/location	Force Intelligence Branch					
Select one of these options	New system / process	X	Change to existing system / process		New use of existing data set	

Explain broadly what the project aims to achieve/what benefits would it deliver.

What would be the consequences of not processing/sharing the data?

You may find it helpful to refer or link to other documents, such as a project proposal

Live Facial Recognition (LFR) is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces against a predetermined watchlist and generates an alert when a possible match is found.

LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database to identify possible matches against persons of interest to Law Enforcement Agencies. Where the LFR application identifies a possible match, the LFR system flags an alert to a trained member of GMP personnel who then decides as to whether any further action is required, such as approaching the individual. In this way, the LFR application works to assist GMP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

Whilst appropriate use of LFR delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing and that the use of LFR has been the subject of much debate. All deployments and considerations to deploy will be governed by a working procedure which will ensure proportionate, legal, accountable and necessary steps are reviewed by an authorising officer who is independent of the LFR deployment itself.

LFR can be a valuable policing tool that helps forces keep the public safe and to meet their common law policing duties, as laid out in **Police Information and Records Management Code of Practice 2023** (PIRM 2023) the policing purpose is to:

- protect life and property
- preserve order
- prevent the commission of offences
- bring offenders to justice
- any other police duty or responsibility arising from common or statute law

The following are illustrative examples where LFR may assist GMP to achieve their policing purposes:

- Supporting the location and arrest of people wanted for criminal offences.
- Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders)
- Supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc)

- Supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

The technical operation of LFR comprises the following eight stages:

Compiling/using existing database of images: The LFR application requires a watchlist of reference images against which to compare facial images from the CCTV feed. For images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template). GMP LFR policy outlines considerations relevant to lawfully compiling a watchlist including determining which persons may be on a watchlist and the sources of watchlist imagery.

Facial image acquisition: A CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the zone of recognition and using it as a live feed. The siting of the CCTV cameras, and therefore the LFR deployment location is important to the lawful use of LFR. The GMP LFR policy and procedure provide considerations relevant to the locations GMP may select to deploy the cameras when using them for LFR.

Face detection: Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

Feature extraction: Taking the detected face the software automatically extracts facial features from the image, creating the Biometric Template.

Face comparison: The LFR software compares the Biometric Template with those held on the watchlist.

Matching: When the facial features from two images are compared the LFR application generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

The Threshold Value GMP will be utilising is 0.64, this is above the threshold recommended to minimise false positive matches and allow greater confidence in matches made. This is in line with the recommendations as laid out by by the College of Policing (CoP) Authorised Professional Practice (APP) for facial recognition and the established best practice currently in use at existing pilot forces (The Metropolitan Police and South Wales Police).

Engagement Officer consideration of matched images

Once an alert has been generated, Engagement Officers who are trained on LFR use will assess the relevant candidate image against the relevant Watchlist image and make a decision as to whether they consider the match to be viable, and if so whether any further action is required.

LFR data destruction

Where an alert is not generated, the biometric templates created in respect of members of the public whose images have been captured by LFR are immediately and automatically deleted.

Where the LFR system generates an alert, the biometric template is deleted as soon as practicable and in any case within 24hrs except to the extent that:

- personal data is retained in accordance with the Data Protection Act 2018, Management of Police Information (MOPI) and the Criminal Procedures and Investigations Act 1996;

- personal data is retained in accordance with the GMP's complaints / conduct investigation policies.

LFR Watchlists are deleted as soon as reasonably practicable and in any event at the end of a deployment and in any case within 24hrs following the deployment.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except to the extent that the footage is retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996;
- in accordance with the GMP's complaints / conduct investigation policies;

To support compliance the LFR system has a full audit capability, and the LFR log is retained in accordance with MOPI. (*The LFR log is a contemporaneous record of the LFR deployment including details of operators undertaking the work, numbers of subjects on the watchlist and the alerts generated by the system for example.)

Data security – The LFR system includes a number of physical and technical security measures.

These include:-

- The transfer process for any Watchlist created is detailed in the GMP LFR Deployment Process Standard Operating Procedures document which ensures all activities, data management and handling of the hardware is carried out in line with agreed processes by all operatives.

- Images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine; this transfer mechanism is required as the LFR software will be installed on a standalone server which is not connected to the main GMP infrastructure. (It is anticipated that from early 2026, the transfer of watchlist data will take place via the GMP network, using GMP infrastructure including VPN, firewall and remote access capabilities.)

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

- The LFR system is physically protected when in use and securely wiped following each Deployment

<u>Watchlists</u>

GMP have a number of different watchlist criteria in line with the current APP for LFR deployment. All watchlists fall into the categories stipulated in the GMP LFR procedure (the "a-f" - as laid out below). Each watchlist is created no more than 24 hours in advance of a deployment but should be refreshed as close as possible prior to any deployment to ensure the information is as up to date as possible.

The watchlist is bespoke for every deployment, limited to the size needed to meet the policing purposes identified and the rationale for the make-up of the watchlist, must be intelligence-led, justified, proportionate and necessary, with the nature of the watchlist recorded prior to each deployment. The criteria for constructs of watchlists must be approved by the Authorising Officer (AO), with any images included being specific to an operation or to a defined policing objective and only when less intrusive means of location have proved unsuccessful. Any images for inclusion on a watchlist, must also be limited to the categories of image of people who are:

- a. wanted by the courts; and/or
- b. suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
- c. subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or
- d. missing persons deemed increased risk; and/or
- e. presenting a risk of harm to themselves or others.
- f. a victim of an offence or a person who the police have reasonable grounds to suspect would have information of importance and relevance to progress an investigation, or who is otherwise a close associate of an individual and that individual would fall within people wanted by the courts and presenting a risk of harm to themselves or others.

Watchlist composition will be restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR deployment. However, an AO may deem it necessary and proportionate to authorise the inclusion of people wanted for the most serious offences to be included in a watchlist, even though there may not be specific intelligence to say where the person of interest might be found.

Watchlists can be amended during a deployment with the ability to manually delete persons, i.e. following a true alert and engagement, the subject can be removed from the watchlist to prevent any duplication of alerts and therefore remove the risk of multiple engagements.

Each deployment of Live Facial Recognition will be subject to a full AO pre-deployment authorisation report which will clearly define the strictly necessary argument for processing personal data, along with setting out clearly, the case for the deployment's compliance with the College of Policing's Authorised Professional Practice of being targeted, intelligence led and time bound and geographically limited. That document should be read in conjunction with this DPIA for a full understanding of the specific processing, risk assessment and mitigations applied.

Watchlists can be created from any GMP owned data set including, but not limited to, CORVUS and PoliceWorks. The locations of general deployments will be based on analysis of crime hotspots rather than any subjectively chosen areas; this will be monitored long term to identify any trends and to assess whether the deployment of LFR itself has had any impact on crime rates in these areas.

Targeted deployments can include large scale events such as football matches, political conferences, music festivals, therefore the locations of these deployments will be determined based on where they are held. The use of this technology is necessary to ensure that GMP is able to effectively and efficiently locate and identify persons of interest who may pose a threat to themselves or wider society. By not optimising the latest advancements in facial recognition technology, the extent to which GMP is able to effectively deliver its law enforcement functions is limited.

SECTION 1:

DPIA Screening Questions: If the answer to all of the questions below is 'No', a full DPIA is not required. In such instances just complete this page and submit the document to the Data Protection Officer / ICRMU for review and approval.

If the answer to any of the questions below is "Yes", a full DPIA should be completed. Submit the completed questionnaire to the ICRMU for review and Data Protection Officer approval.

Does the change initiative involve any of the following:		**Yes**	**No**
1.	Use systematic and extensive profiling or automated decision-making to make significant decisions about people? *Includes evaluation or scoring of individuals*		X
2.	Process special category data or criminal offence data on a large scale? *Special category data includes: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; data concerning health; data concerning a person's sex life or sexual orientation)*	X	
3.	Systematically monitor a publicly accessible place on a large scale? *Includes CCTV and other surveillance systems*	X	
4.	Use new technologies? *Includes innovative technological or organisational solutions*	X	
5.	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? *Whether or not this is on a large scale*	X	
6.	Carry out profiling on a large scale? *Even if this doesn't involve automated decision-making*		X
7.	Process biometric or genetic data? *Whether or not this is on a large scale*	X	
8.	Combine, compare or match data from multiple sources?	X	
9.	Process personal data without providing a Privacy Notice directly to the individual? *Even if the lawful basis for processing suggests a Privacy Notice is not required*		X
10.	Process personal data in a way which involves tracking an individual's online or offline location or behaviour?		X
11.	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?		X
12.	Process personal data which could result in a risk of physical harm in the event of a security breach?	X	
13.	Does the scale of the project alone justify completion of a DPIA for quality assurance purposes?	X	

Conclusion:	Yes	No
Is there an intention to complete a DPIA?	X	

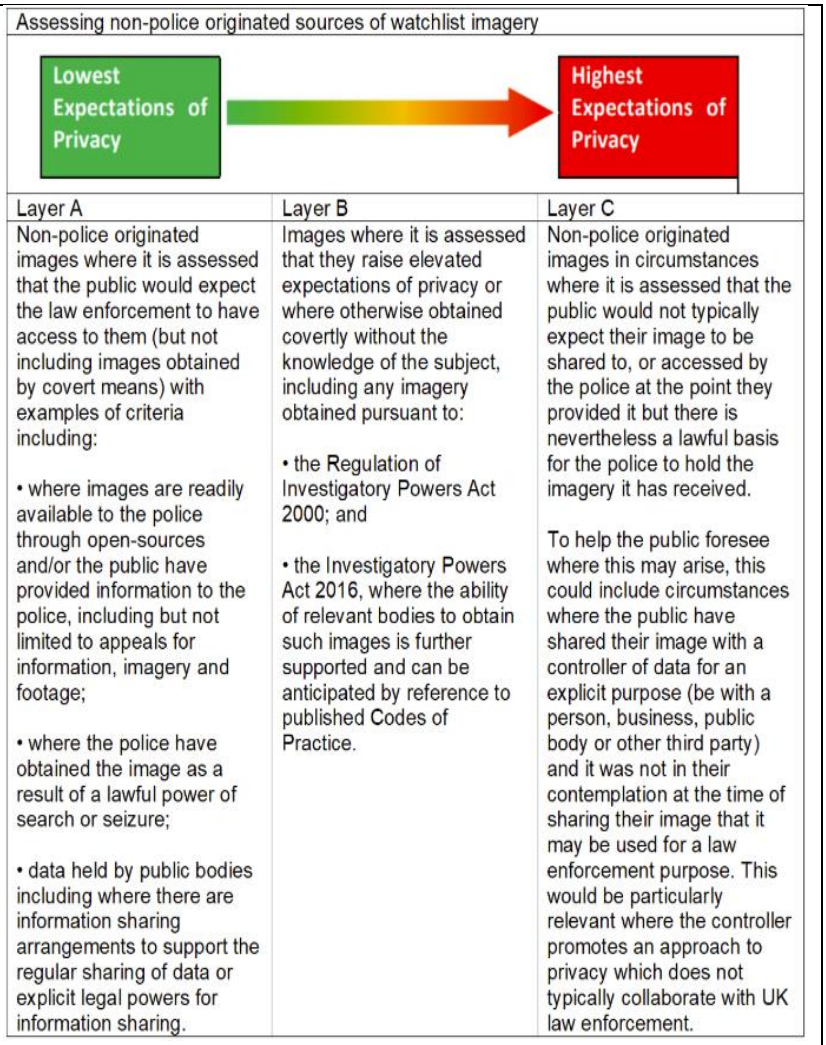
If all answers above are No there is no requirement to continue to Section 2. Please email the assessment to the ICRMU via email to: dataprotection@gmp.police.uk

If any answers above are Yes please continue to complete Section 2 below before emailing the assessment to the ICRMU as above.

SECTION 2: Please refer to the guidance notes on completing a DPIA

Step 1: Identify the need for a DPIA	
1.0 Summarise why you identified the need for a DPIA	LFR is a real-time deployment of facial recognition technology, which compares live camera feed(s) of faces against a pre-determined watchlist and generates an alert when a possible match is found. Whilst appropriate use of LFR delivers clear value to UK law enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing, a particularly sensitive form of personal data, and is considered high-risk processing. This DPIA assesses GMP's intended use of LFR technology for law enforcement purposes to ensure that its use operates within the confines of data protection and human rights laws, whilst recognising the impact on individuals and their reasonable expectations of privacy.
Step 2: Describe the processing	
2.1 How will data be collected or obtained and how will the data be used?	The decision to authorise an LFR deployment will be tightly governed. Once a consideration for LFR deployment has been established, a full AO pre-deployment authorisation report will be compiled. The report will clearly define the strictly necessary rationale for processing personal data, along with setting out clearly, the case for the deployment's compliance with the College of Policing's Authorised Professional Practice of being targeted, intelligence led and time bound and geographically limited, has been carried out. <u>Deployment record</u> - the written authority document and the LFR cancellation report which details the date & time the operation was stood down. This sets out the details of a proposed deployment including – but not limited to: a. location b. dates and times c. deployment and watchlist rationale d. legal basis e. necessity f. proportionality g. safeguards h. watchlist composition i. authorising officer j. resources k. relevant statistics l. outcomes m. summary of any issues A liveried van will be used for LFR deployments containing a GMP laptop which will be installed with the NeoFace software, produced by Nippon Electric Company (NEC). A watchlist of predefined images generated from police systems is loaded

	into the software ahead of a deployment, from which biometric templates are created from the images. The watchlist is compiled from data already held by GMP through lawfully held images such as custody images of individuals and/or obtained from other means, which could be family/friends for high-risk & medium risk missing persons, social media profiles and from the police evidence gathering team or additional sources if required for a particular operation. Where police originated images, other than custody images, are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist to meet a policing objective and the proportionality of using such images on an LFR System. There will be occasions where no image is held by GMP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image. Non-police originated images are images which have not originated from law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness.



Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular which layer of intrusiveness the image is attributable to and the factors above.

Further information can be found Watchlist | College of Policing

The van used for a deployment is fitted with two CCTV cameras and a live CCTV system which captures the images of individuals passing through the zone of recognition where the van is located. When an individual's image is captured via the CCTV feed, the NeoFace system will carry out "facial extraction" and create a biometric template from the facial image.

Faces per frame - a configurable setting within the software that determines the number of faces that can be analysed by the LFR application in each video frame. - GMP will be using the standard 10 faces per frame rate of analysis on operations, this can be increased however will impact speed of matches being made.

The NeoFace software will then compare the two biometric templates (the template created from the watchlist and the template from the CCTV feed).

When the facial features from two images are compared, the LFR application generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of the algorithm varies dependent on demographic factors. As a result, GMP has had regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST), who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by the creator of the NeoFace Live Facial Recognition technology, Nippon Electric Company (NEC). The National Physical Laboratory (NPL) has also undertaken specific operational testing and have determined the most appropriate minimum threshold setting.

For GMP, the threshold setting will ordinarily be equal to or above the value where no LFR System bias is detected (0.64 with the current LFRalgorithm). The Threshold value may be lowered based on the intelligence case with a full rationale detailed in the GMP LFR Application / Written Authority Document.

Trained members of police personnel will review the alerts and decide as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

In the event that a trained officer decides to engage with a data subject following an alert, this will be carried out in the usual professional policing manner.

<u>Blue Watchlist</u>

. A “blue watchlist” will also be created.This is a “test” watchlist that comprises known persons that can be used to test system performance. This will consist of police officers / staff, who will be ‘seeded’ into the crowd and will walk through the Zone of Recognition at the start of a every deployment to measure the True Recognition Rate.

<u>Register of Deployments</u>

Any deployment of LFR must be recorded on a centrally held register. This register will record:

a) name and rank of the AO and command team.
b) date, time, duration, and locality of Deployment.
c) watchlist composition statistics (not including any personal data);

	d) number of Alerts, broken down as True Alerts and False Alerts, including: (i) perceived age range (ii) perceived sex (iii) perceived race (by reference to Policing IC Code) e) number of engagements and their results. <u>Post-Deployment</u> A record of deployments will be published on the GMP website. This will confirm for each Deployment: i. Deployment location ii. Date of the Deployment iii. Duration of the Deployment iv. Whether the Deployment was to a crime hotspot, missing person hotspot, to support a PSO and/or following specific intelligence. v. Watchlist size vi. The minimum threshold setting. vii. Total Alerts viii. The number of Confirmed True Alerts and Confirmed False Alerts, ix. The number of unconfirmed True Alerts and False Alerts, x. The False Alert Rate xi. Estimated faces passing the LFR system.
2.2 Will you be sharing data with anyone? *You might find it useful to use a flow diagram or another way of describing data flows*	GMP will not routinely share any personal information processed during its LFR activities with external parties. However, should the LFR system generate an alert, the subsequent process might typically involve GMP personnel using policing databases and other intelligence systems to carry out any further action. This subsequent action could possibly result in GMP sharing personal data with other police forces, law enforcement agencies and / or partners in accordance with routine information sharing arrangements, depending on the unique set of circumstances attributed to the individual in question. No specific details about individuals will be publically shared on GMP's website, only statistical information relating to the deployments The deployment record or written authority record will not be shared publicly on GMP's website, however the deployment statistics and Register of Deployment will be published following each deployment. All record types, laid out above, are subject to disclosure to the Deputy Mayor's office, Indepedent Office of Police Conduct (IOPC), The Biometrics and Surveillance Camera Commissioner and the Information Commissioner's Office

	should the need arise through complaint or auditing processes and procedures.
2.3 How will the data be transferred? *i.e. Physical data (paper format)* *- collected/hand delivered in person* *- postal (i.e sent via special delivery, double enveloped).* *i.e. electronic data* *- via secure system (i.e Egress – secure email).* *- Files/disc/pen drives (encrypted – password protected)* *Please refer to Government Security Classifications (GSC) Policy & Procedure*	The NeoFace LFR system will operate on a standalone server on a laptop located in the van used for deployments. The computer hosting the LFR system will not be connected to the main GMP network. The Watchlists including images will be stored on an isolated GMP network drive to which only LFR operators have access. From the secure network drive, the watchlist will be copied to a secure, encrypted USB device; an AES-CBC 256-bit full disk hardware encryption engine. The download of the watchlist to the USB device will take place on GMP premises. The watchlist will be uploaded to the computer in the LFR van once the van system tests have been completed. The content of the USB device will be deleted immediately after the watchlist has been downloaded into the LFR system. The USB device will then be stored in the key safe within the vehicle. The USB will have an audit trail of deployment paperwork and will need to be signed in and out by officers responsible for completing each stage of the data transfer of the watchlist from the GMP network to the LFR system in the van.. Access to the USB device containing the Watchlist is limited to those with a need to use it, who have completed GMP's LFR training. There is a procedure for the handling of the USB which covers all security arrangements.
2.4 How will the data be stored? *i.e. physical data – locked away in draw/cupboard* *electronic data – stored on a secure network/server with logon/password credential, files/disc/Pen drive encrypted*. *Please refer to Government Security Classifications (GSC) Policy & Procedure*	The collection of personal information is via CCTV cameras connected to the laptop / LFR system. The application extracts a face from CCTV footage (known as a probe image) creates a biometric template and then compares it against the biometric template created from the watchlist source data. The biometric templates from the source data (watchlist) is created when the watchlist is uploaded into the system at the start of a deployment. Each unique watchlist created for each deployment is stored temporarily on the GMP isolated drive for a maximum of 24 hours following the end of the deployment. As described above, the watchlists are also temporarily stored on an encrypted and password protected USB device to enable the transfer of data to the LFR system which is operated in the van. The biometric templates created from the watchlist are stored in the LFR system software for no longer than the duration of the deployment, and 24 hours maximum. Once the watchlist is uploaded to the LFR Van and checked, the USB stick will be reformatted immediately. On completion of the deployment the watchlist will be deleted from the computer within the LFR van and the operator will be required to updated the deployment log to confirm this action has been completed. The deletion of the watchlist and the formatting of

	the USB drive will be undertaken by two officers who will countersign the completion of each task. The LFR system does not save images from the live CCTV feed, only a particular face if a possible match is made against a candidate image along with a wider CCTV frame from which the probe image was extracted. Information pertaining to alerts are stored on the system for the remainder of the deployment. After the deployment, the LFR operator will download the CCTV footage from the van, which will need to be checked for completeness. This will then be uploaded to Evidence.com via Axon under the heading Public Order/EGT- which is the current metadata header within evidence.com. It will be marked with restricted access and will be kept for 31 days, after which point it will be deleted automatically. Should the footage be required for further use prior to deletion (either policing or professional standards reviews) then it may be accessed for these purposes, with access provided by the LFR team once approved. . The deployment record or written authority record and Register of Deployment will be stored in the GMP LFR team secure SharePoint folder. The record of deployment statistics will be published on GMP's website and also stored on GMP LFR's team secure SharePoint drive. BlueWatchlist - The images of those who have signed the consent form are held on a shared database (within the LFR MS Teams area) which will have restricted access permissions; this will be stored centrally to allow it to be updated as necessary. Each LFR Operator will have to sign an explicit consent form when they attend their LFR training, which will be stored in the private LFR Teams channel. A spreadsheet will show when each operator completed their training which will be reviewed every 12 months. Consent can be withdrawn at anytime..
2.5 What will be the retention of the data? *i.e will data be retained as per MOPI (see link) or other retention schedules / statutory requirements that are applicable to the data?*	The Biometric Templates created by the system during the deployment via the CCTV footage which are not deemed a possible match against the watchlist and do not create an alert will be automatically deleted by the LFR system. Where there is a Possible Match, this will generate an Alert, which is displayed to the LFR Operator. If a Possible Match is made, three thumbnail images will be saved within the application along with the related metadata. The first is the Candidate image, the second is the face extracted from the CCTV and the third being the CCTV frame from which the Probe Image was extracted.

	Where the LFR system generates an Alert, all related personal data is deleted once the deployment is convened (within 24 hours). except to the extent that: (i) Personal data is retained in accordance with the Data Protection Act 2018, PIRM 2023 and th Criminal Procedures and Investigations Act 1996; (ii) Personal data is retained in accordance with the GMP's complaints / conduct investigation policies. All CCTV footage generated from LFR Deployments is deleted within 31 days, except to the extent that the footage is retained: (i) in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996; (ii) in accordance with the GMP's complaints / conduct investigation policies; (iii) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data. After the deployment, the LFR operator will download the CCTV footage from the van, they will then upload this to Evidence.com via Axon under the heading Public Order/EGT. It will be restricted access and will be kept for 31 days, after which point it will be deleted automatically. Should the footage be required for further use prior to deletion (either policing or professional standards reviews) then it may be accessed for these purposes, with the LFR team can providing access. Watchlists and associated metadata are deleted as soon as reasonably practical after a deployment or at the latest within 24 hours of the conclusion of the deployment. LFR Operator and Engagement Logs are retained in line with the MOPI retention periods. Each deployment will have its own deployment log with a unique reference number which is signed out and signed back in. The retention of the three specific records (deployment record / Authority record, the Register of Deployment and the deployment statistics) are retained indefinitely. The specific information held on the post-deployment register relating to any arrests or engagements, will contain personal data such as, nominal reference number, the offence, gender and ethnicity. Albeit, this is Personal data held on this register, this is namely statistical and only accessible to the approved

	LFR team, who have undertaken training, and the data is pseudonymised. Staff would be required to access other GMP systems with the nominal reference number to reveal the individual's identity. Consent forms from LFR operators who consent to their data being used as part of the BlueWatchlist will be retained indefinitely and reviewed on an annual basis, to ensure that the consent remains current and relevant. The BlueWatch List images will be stored indefinitely, for training and quality-assurance purposes.
2.6 How will the data be deleted/disposed of? *i.e. those parties/partners processing/sharing data with, do they have their own disposal policy?* *Will information be returned back to the data controller (GMP) for destruction?* *Will data be disposed of inline with Government Security Classifications (GSC) Policy & Procedure*	Watchlists within GMP infrastructure are updated every 24 hours meaning the data held within them remains up to date.. Biometric data created by the system during a deployment via the CCTV system will be automatically deleted if there is no match to data on the watch list, and at the end of the deployment if there is a match. The watchlist data and the accompanying biometric data created from the watchlist used for the deployment will be manually deleted by an LFR operator immediately following the conclusion of a deployment. All CCTV footage generated from LFR Deployments is automatically deleted on Evidence.com within 31 days, except to the extent that the footage is retained: (i) in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996; (ii) in accordance with the GMP's complaints / conduct investigation policies; (iii) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.
2.7 What types of processing identified as likely high risk are involved? *Please see link to ICO website explaining what constitututes high risk processing*	LFR deployments entail the large scale processing and matching of personal data, including special category data and biometric data, and personal data relating to criminal convictions and offences, using innovative technologies.

	The processing also involves systematic monitoring of a publicly accessible area on a large scale. The processing involves the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)
2.8 What types of data subject will be involved? *i.e. offenders, victims, GMP employees, children, vulnerable adults etc*	Police originated images that may be included on a watchlist include custody images of individuals and/or police originated images other than custody images of people who are :- a. wanted by the courts; and/or b. suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or c. subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment; and/or d. missing persons deemed increased risk; and/or e. presenting a risk of harm to themselves or others; and/or f. who are a victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual and that individual themselves would fall within paragraphs (a) – (f). **Persons who may be included on a watchlist – definitions:** ***"Wanted by the courts"*** - This term includes those with outstanding arrest warrants or who are otherwise required by the courts. 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. ***"Missing persons deemed increased risk."*** - This term is as per the College of Policing definition of medium risk (or above) that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.

	"Presenting a risk of harm" - Mitigating the risk of harm to themselves or to others will need to have a legal basis for action under a policing common law power. 'Harm' can include a risk of harm arising in relation to a person's welfare and/or a financial harm including as a result of fraud or other dishonesty. It can also include 'Harm' in the context of posing a risk to national security. The risk of harm will be informed by the intelligence case and/or the considerations set out in the applicable LFR form. This will need to inform the AO as to how the individual or group of individuals present(s) a risk of harm to themselves or to others and how a) using LFR to facilitate their location is necessary to manage the risk of harm identified; and b) why the significance of the harm identified means it is necessary for the police to take action in order to manage the risk. The applicant would also have to demonstrate the proportionality of any inclusion on a Watchlist. This would include considering: a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and b) the importance of locating the person or people sought with reference to the threat, harm and which the addition to the Watchlist addresses; c) whether the significance of the threat, harm and risk identified, which inclusion on the watchlist would address outweighs any expectations of privacy. ***"Victim of an offence, or a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual."*** This criteria includes a victim, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within (a) – (e) of the categories that may be deemed appropriate for inclusion within an LFR Watchlist.

	The threshold for any Watchlist inclusion is high and the use of the category will be by exception; the necessity for inclusion must be based on a specific intelligence-case with the need for the inclusion on a watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to able to demonstrate to the AO's satisfaction: a) why the inclusion of each victim, person reasonably suspected of having information, or close associate is necessary to help locate the person who is wanted by the courts and/or the police; and/or b) why locating each victim, person reasonably suspected of having information, or close associate person is necessary to advance the policing investigation; and/or c) why locating each victim, person reasonably suspected of having information, or close associate is necessary to ensure their safety and/or the safety of others. The applicant would also have to demonstrate the proportionality of any inclusion on a watchlist. This would include considering: a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and b) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses; c) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any inclusion on the watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others. Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a policing objective and the proportionality of using such images on an LFR System.

The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria stipulated in this GMP LFR procedure and be specific to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:

Requirement	Rationale
Intelligence: Watchlists must be driven by a policing need and based on the intelligence case. The intelligence case must be current and reviewed before each Deployment.	This intelligence-driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR deployment
Images sources: Watchlists must only contain images lawfully held by police with consideration also being given as to: i) the legal basis under which the image has been acquired; and ii) the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.	This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance. Additionally policing has a responsibility to avoid compromising policing tactics or exposing sources to risk – this requirement covers this point
Image selection: Watchlists must only use images where all reasonable steps have been taken to ensure that the image:	This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located.

i) is of a person intended for inclusion on a given Watchlist; and; ii) is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the proposed image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator).	The GMP SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.
Watchlist currency: Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment	This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours
Watchlist design: Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.	This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated.

Children and Vulnerable People

It is possible that there will be processing of children or vulnerable groups, processes will remain as described throughout this DPIA and other associated GMP LFR documents. However, each deployment must specifically identify and document whether the Watchlist contains children

who are believed or suspected to be aged under 18-years-old and under 13-years-old.

If LFR is to be used to locate children aged under 13-years-old, specific regard should be given to anticipate LFR application performance issues.

Where an Alert occurs relating to a vulnerable person or a child suspected or believed to be under the age of 18, the Engagement Officers should take all reasonable steps to ensure the child/ vulnerable person understands what is being said to them. This is particularly pertinent to children under 18, persons who are vulnerable through diminished capacity or understanding or people who are unable to understand or communicate effectively in English. If there is any doubt that the child/ vulnerable person understands what is being explained to them, the Engagement Officer must take reasonable steps to ensure the understanding of the child/ vulnerable person and to bring relevant information pertaining to LFR use to their attention.

Where Alerts are generated relating to children or vulnerable people who are included in the Watchlist, or the Subject of an Alert is accompanied by a child or vulnerable person, force safeguarding procedures should be initiated. This is especially pertinent for Children and vulnerable persons (as defined by College of Policing). It is recognised that children under the age of criminal responsibility may be used by older children and adults to hold illegal items such as drugs and weapons and, in some cases, firearms or to undertake criminal activity for the criminal benefit of others.

Children under 10 should only be included in Watchlists for LFR in exceptional circumstances and their safeguarding and welfare should be the immediate priority of the Engagement Officer.

Police officers or staff

Officer and staff are placed on to the Bluewatch list to test system performance. Officers / staff are 'seeded' into the crowd and will walk through the Zone of Recognition at the start of a every deployment to measure the True Recognition Rate.

Other

Members of the public who cross the path of the CCTV camera and have a biometric template taken by the software will be processed against the watchlists.

2.9 What category of personal data will be processed, basic personal identifiers (name, d.o.b, address etc or will it also include special category or criminal offence data?

Special Category Data refers to:

- *personal data revealing racial or ethnic origin**;***
- *personal data revealing political opinions**;***
- *personal data revealing religious or philosophical beliefs**;***
- *personal data revealing trade union membership**;***
- *genetic data**;***
- *biometric data (where used for identification purposes);*
- *data concerning health;*
- *data concerning a person's sex life; and*
- *data concerning a person's sexual orientation**.***

Each watchlist entry will include the following fields:

• Watchlist name
• Gender
• First Name
• Middle Name
• Last Name
• Warning Markers
• Date of Birth (DOB)
• Alert Type
• Unique Reference No (URN)
• Reported Time
• Info (contextual information in relation to the "wanted" status)
• RMS ID (the URN reference in the Record Management System)
• PNC ID (Police National Computer) ID
• BCU (Basic Command Unit)
• Class (Wanted warrant, wanted crime)
• Crime Type
• Owner
• Date Image
• Image

Those on a LFR Watchlist - the following data being necessary to construct the Watchlist and/or operate the LFR system to locate Persons of interest and provide actionable information to Engagement Officers in order to respond to Alerts	**Those who pass within the relevant LFR Zone of Recognition – the following data being necessary to operate the LFR system and to compare those passing through the Zone of Recognition to the LFR Watchlist.**

• Subject name
• Facial image, and from/associated with that facial image:
  ○ Biometric facial image template
  ○ Recorded (or if unknown, perceived) gender
  ○ Recorded (or if unknown, perceived) age/date of birth
  ○ To the extent arising from looking at the image, any perceived religious or philosophical beliefs, perceived ethnicity, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).
	• CCTV footage of data subjects passing through the Zone of Recognition
	• Available to GMP via the use of the CCTV footage:
	  • Biometric facial image template for alerts only. Biometrics for non-alerts are deleted instantly.
	  • Perceived gender
	  • Perceived age
	  • Perceived height
	  • Metadata (i.e. location, date and time the footage was captured)
	  • Any perceived points concerning a relevant disability/gender transition

• Criminal offence data or information concerning why they are missing in order to confirm why the subject is a Person of interest (which, in particular in the case of MAPPA nominals, may include data concerning the individual's sex life) • Warning markers (e.g. known to possess weapons) • Alert Type • Unique Reference No. (URN) • PNC ID Note: Further personal data would be available to, and recorded by officers using GMP local systems during the Engagement process. This is not data processed by way of LFR deployment itself, and is instead relevant to the conduct of officers in the normal course of their duties	On some occasions any perceived religious or philosophical beliefs, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).

Alongside the images within the watchlist there will be data appended to the image that will include:

- Name
- DOB
- Gender
- Warning Signals,
- Nominal reference number
- And the reason they have been included on to the list – this will usually incorporate criminal offence information however, this may on occasion be used for safeguarding purposes, such as missing persons.

Additional safeguards relating to protected characteristics

i. Following on from the Bridges case, in December 2020 the then Surveillance Camera Commissioner (SCC) published the best practice guidance document 'Facing the Camera'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist.

ii. Any controls, mitigations and processes identified by GMP in GMP's LFR documents reflect GMP LFR system's performance and GMP's particular use cases for LFR.

iii. GMP has confidence in the LFR System's performance, particularly in relation to gender, age and race.

iv. GMP recognises that regardless of performance considerations, it should take particular care when considering and publishing details relating to age including the protection of children – particularly the very young, persons with disabilities and those who have and/or are undertaking a gender reassignment. This is because:

a. There may be different privacy expectations around the use of LFR for persons with these protected characteristics and that these can be particularly relevant in relation to these people given their potential vulnerability.

b. GMP recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.

v. Documenting composition - GMP provides that each deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be:

a. aged under 18-years-old;

b. aged under 13-years-old;

c. a person with a relevant disability (in this context those with a disability defined in Section 6(1) of the Equality Act 2010 which may impact on performance of the LFR system).

d. a person who has undertaken a gender reassignment and it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment.

vi. Safeguards regarding composition - the following outlines further, specific safeguards that apply to the composition of the Watchlist:

	Age – Under 18	Age – Under 13	Disability	Gender Reassignment
Circumstances				

	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 18-years-old	LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability	LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment

Safeguards		
Necessity	Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with LFR Documents with a particular focus on ensuring the necessity case is fully made out.	
Watchlist Images		There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.
Legal Advice		Specific advice must be sought from Legal Services and the GMP LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.
Technical Advice		Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.
	Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be blocked from the camera's line of sight.	Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.

NB - Generally, studies have shown that young children, up to the age of 13 are both harder to correctly recognise (lower True Positive Identification Rate) but also harder to distinguish between (higher FPIR). The higher FPIR may lead to more False Alerts being generated against young children if there is an image of a young person in the Watchlist.

2.10 How much data will you be collecting, using and how often? How many individuals are affected? *Provide figures if known and timescales (i.e. monthly, once etc)*	The exact amount of data is difficult to estimate and depends on a variety of factors during a deployment which affect the number of persons passing the camera zone of recognition and having a biometric template taken. These factors include location, camera positioning, time of day and duration of deployment. It is anticipated that for each deployment, approximately 1000 to 5000 data subjects could pass through the camera zone of recognition but there will be deployments where this figure is less than 1000 or more than 5000. Frequency of deployments cannot be estimated as they will be intelligence led and this depends on the intelligence picture, demand for deployments and whether the deployments are authorised. In terms of the watchlist data, it is estimated that the watchlists will not exceed 15,000 data subjects.
2.11 How long do you expect this initiative to last?	The LFR project will be an ongoing initiative. For specific LFR deployments, the AO should define the date, time, location and duration the deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the deployment. It is not anticipated that a deployment should exceed 7 days in length. Should the need to deploy continue beyond 7 days, a further GMP LFR Application / Written Authority Document must be sought. This approach ensures that the use of LFR is proportionate and kept under review.
2.12 What geographical area does it cover? *i.e. the whole of Greater Manchester, one District, etc?*	For the most part, the deployment will be within Greater Manchester boundaries. However, the intention is for GMP to have ownership of the LFR vans and allow neighbouring forces the opportunity to utilise this innovative technology when there is necessity and proportionality to do so. As such, these vans and the specific technology within them have the capability to be utilised outside GM boundaries and within neighbouring Northwest Forces and on a national scale.. Should this occur, the forces procuring the services of GMP and the LFR technology will be responsible for compiling their own watchlists and will be become the data controller for operations. GMP will assume the role of a data processor for these arrangements. For GMP deployments, the AO should define the date, time, location and duration of the authorised deployment based on

	the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the deployment. The intelligence case, policing purpose to include a person on a Watchlist, Community Impact Assessment and the environmental factors relevant to a potential deployment location will substantially inform the potential locations for LFR Deployments. Deployment locations will be determined by there being reasonable grounds to suspect that the proposed deployment location is one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any selected deployment location should be recorded and be capable of being considered and evaluated by an objective third person which forms part of the authorisation process undertaken by a Superintendent. The selection of a particular deployment location may further be supported by: a. policing information or intelligence about a proposed Deployment location including if there is an increased public safety risk and/or need to provide public reassurance at the location; and b. the ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so. When reviewing a potential Deployment location, AOs must also consider: a. Those who are likely to pass the LFR system and the reasonable expectations of privacy they may have as a whole at that location (some places by their nature attract greater privacy expectations than others) b. The number of cameras used by the LFR System to ensure the size and scale of the deployment enables those on a watchlist to be effectively located without disproportionately processing biometric data. c. If a proposed deployment location attracts particular concerns by reference to those expected to be at a particular location (for example hospitals, places of worship, centres for legal advice, polling stations, places of education, lawful assemblies) there may have a greater expectation of privacy and/or people may feel less able to express their views or otherwise attend the location area.

	Where it is practicable to identify a person of being responsible for a proposed deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate. Where privacy or other human rights considerations are identified in relation to a particular deployment, the AO needs to consider the necessity to deploy LFR to that particular location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is necessary (with the processing of data at that site being strictly necessary), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR System against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.
2.13 How much control will the data subject have over the data being processed? Would the data subject expect you to use their data in this way?	Deployments will be publicised in advance and will be highly visible (liveried vehicle and signage/posters), use of engagement officers at locations. Once a data subject is in the zone of recognition and their image is processed, they will have no control over the processing of their data. Some data subjects may choose to avoid the zone of recognition or cover their face so that their image cannot be used by the CCTV feed to create a biometric template. The data subject may expect GMP to include the use of facial recognition technology in the discharge of its policing duties, but GMP recognises that some data subjects may not expect their data to be used for this purpose.
2.14 GMP require a cyber security assessment to be completed; Please provide an email address and full company name; *We require your participation in our third-party security risk management programme. This process gives us assurance that our suppliers have implemented an appropriate level of security controls to protect themselves, and us, from cyber incidents.* ***How?*** *GMP use Risk Ledger to manage this process. Risk Ledger is a third-party platform that allows suppliers to complete one comprehensive security assessment which can be shared with any other client who requires an assessment - not only does this save*	NEC Software Solutions UK Limited 1st Floor, iMex Centre, 575-599 Maxted Road, Hemel Hempstead, HP2 7DX dpo@necsws.com NEC has been awarded the contract with GMP via Blue Light Commercial. A cyber security assessment has been completed and the company and is registered on Risk Ledger.

organisations a lot of time but helps to speed up their sales cycles. We are committed to making this process as pain free as possible for our suppliers, and Risk Ledger helps us to do that. Risk Ledger has strict data privacy and security policies, which can be found in their Terms and Conditions and Privacy Policy. For further information on Risk Ledger please look at Risk Ledger's FAQs. ***What next?*** *The third party will receive an email from the email address no-reply@riskledger.com asking them to sign up to their platform and complete an assessment. Once submitted, we will have visibility of the results. GMP might raise discussions with them within the platform once we begin our review. If you have any questions about the process please message support@riskledger.com.*	
2.15 Are there any current issues of public concern that you should factor in? *i.e. this could include the impact on the public or where there is no impact then state the benefit on the public*	The use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing. The Information Commissioner's Office (ICO) has undertaken research into public attitudes to LFR, and recently published its findings: Understanding the UK public's views and experience of biometric technologies. The ICO has found that most people recognise there is an impact on their right to privacy, but they are also broadly supportive of the use of LFR; support is strongest for use cases with a very clear rationale and clear public benefit. Use of LFR by police forces in England has attracted local and national media attention with a mixture of positive and negative reporting. Campaign groups such as Liberty and Big Brother Watch have and continue to campaign against police use of facial recognition.. In 2020 the court of appeal found in favour on two counts of a claimant against South Wales Police's (SWP) use of LFR. One of the counts related to concerns around the accuracy of the algorithms used and a potential bias against some individuals' protected characteristics. Since then SWP and the Metropolitan Police Service (another use of the Neoface technology) have had the algorithms they use tested by an independent agency (for more info see GMP LFT Policy and Equality Impact Asessment documents).

	The following principles will be adhered to during an LFR deployment: i. except in exceptional operational cases, where doing so would undermine objectives or operational imperative of the deployment (for example, in cases of urgency or where it would compromise other policing tactics), the public should be notified of LFR deployments in advance. ii. Measures should also be taken during the deployment to ensure the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed. In addition to the use, uniformed officers and marked vehicle(s), other steps for applicants to consider in the context of their proposed deployment location include the use of signage placed in advance (outside) of the Zone of Recognition and/or the provision of information leaflets. iii. In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any deployment is overt, the objectives for the deployment and its use of a policing tactic will also be relevant if the policing need to deploy is to be realised. For example, unduly extensive signage may undermine the effectiveness of a deployment seeking to locate persistently outstanding offenders. By comparison a deployment seeking to protect a site or particular event may merit multiple levels of signs and the proactive distribution of leaflets to deter criminality. iv. 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. GMP staff deployed must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics. v. 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 GMP LFR operational team livefacial.recognition@gmp.police.uk.
2.16 What is the intended effect on data subjects whose personal data you are processing?	Persons who pass through the Zone of Recognition for an LFR deployment will have their personal data processed by means of a biometric template taken from the CCTV image of their face which will then be processed by comparison to biometric templates from watchlists. If there is no match and therefore no alert generated the image and template will be automatically deleted immediately. However, if the comparison returns an alert with a similarity score above the set threshold, it will be reviewed by the LFR Operator and LFR Engagement Officer, who will make a decision whether to engage with the subject or not. If engagement ensues the stop will follow usual lawful policing procedures. The effect of this process is that persons of interest are successfully identified and intercepted by the police, in a

	proportionate and justified way in line with law enforcement policing powers.
Step 3: Consultation process	
3.1 Describe when and how you will seek the data subject's views or justify why it's not appropriate to do so. What information will you give data subjects; is the processing covered either by GMP's (see link below) or another organisation's privacy notice? https://www.gmp.police.uk/hyg/fpngmp/privacy-notice/ *If not you may be required to complete a privacy notice (PN) (template of PN obtainable from ICRMU)*	The data subjects will be persons passing through the LFR deployment zone of recognition. Various documents relating to GMP's use of LFR will be made available on GMP's website (including but not limited to, the LFR privacy notice and Appropriate Policy Documents, GMP's LFR policy and procedure documents and publication of data from previous deployments and dates of future deployments). It is not appropriate to obtain data subjects' consent for this type of data processing activity. During a deployment engagement officers will speak to members of the public about LFR, address any concerns and signpost them to further information available on GMP's website.
3.2 Who else do you need to involve within GMP, or in the case of partners, their organisation? Do you plan to consult other subject matter experts? *i.e.* • *Info. Compliance & Record Mgt Unit -ICRMU (Data Protection) – dataprotection@gmp.police.uk* • *Information Security Team – (InformationSecurity@gmp.police.uk)* • *The Information Services Branch and systems administrators who will can provide access to GMP system(s)* • *Vetting unit – if having access to GMP systems/premises etc?* • *Procurement / HR / Legal Services?*	A Facial Recognition working group has been set up in GMP chaired by the Detective Chief Superintendent within the Force Intelligence Bureau (FIB). The group includes representatives from the GMP Legal Services, Information Management and Data Directorate, Information Technology and Digital Directorate, Crimal Justice &Custody Branch, Procurement and a representative from the District Senior Leadership Team. Consultation has taken place with key stakeholders and this is an ongoing process which will be documented on GMP's LFR Equality Impact Assessment. GMP's Facial Recognition Working Group includes representation from GMCA. The Greater Manchester Deputy Mayor has been briefed on the project and supports its implementation. Further consultation is ongoing with the Greater Manchester Ethics Committee and GMP Independent Advisory Group.
3.3 Do you need to ask the other parties/partner/processors to assist/comply? *i.e is this arrangement governed by a contract / Data Processing Agreement / Information Sharing Agreement / IT Systems Access Agreement / Memorandum of Understanding* *Legislation / policy & procedures* *Reviews?*	NEC Software Solutions' processing of GMP's data for the purposes of fulfilling their contractual obligations as the supplier of the LFR technology will be governed by data processing conditions included with the contract.

Step 4: Assess necessity and proportionality	
4.1 What is your lawful basis for processing? Is the processing subject to a statutory act/legislation?	Any force LFR system will need to comply with Surveillance Camera Code of Practice and the 12 guiding principles: Surveillance Camera Code of Practice The College of Policing Authorised Professional Practice Live facial recognition: consultation document highlights several key legislations that are often relevant and are to be considered when utilising and deploying facial recognition technologies. These are as follows: • Common Law Policing duties • Police and Criminal Evidence Act 1984 Code D • The Human Rights Act 1998 • The Data Protection Act (DPA) 2018 • UK General Data Protection Regulation (UK GDPR) • The Protection of Freedoms Act 2012 • The Equality Act 2010 GMP's use of LFR, will fall in to both the Law Enforcement purpose of the Data Protection Act 2018 and UK GDPR. **Part 3 Data Protection Act 2018** Section 31 - **The law enforcement purposes** 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. Where GMP is processing data for the law enforcement purposes described above, the lawful basis for processing is provided in: Section 35(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair. Section 35(2) 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 (b)the processing is necessary for the performance of a task carried out for that purpose by a competent authority. Section 35(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted in subsections (5). Section 35(5)(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.

SCHEDULE 8
1 Statutory etc purposes
2 Administration of justice
4 Safeguarding of children and of individuals at risk

Part 2 Data Protection Act 2018

UK GDPR - For General Purpose:

Where GMP is processing data for a general purpose, such as safeguarding, missing persons and the Blue Watchlist to test system performance, the lawful basis will fall into either:

Article 6(1)(a) - the data subject has given consent to the processing of his or her personal data for one or more specific purposes

Or

Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;.

The relevant article 6 condition will be met with the relevant Article 9 conditions. These will be:

Article 9(2)(a) – the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,

Processing under Article 9(2)(a) will be limited to processing participating staff images for the purpose of validating LFR technologies.

Where explicit consent is sought in the limited circumstances in which it is required (e.g. LFR operators participating in the BlueWatchlist testing), the consent is unambiguous and for one or more specified purposes, is a freely given, is a fully informed affirmative action which is recorded and managed to ensure the facilitation of individual rights, including withdrawal of consent. LFR operators provide their consent during the training programme they undertake prior to any deployment. . Although the consent provided by officers and staff does not 'run out' it does degrade over time and as such the consent is reviewed when an officer completes an LFR refresher course to ensure that the consent is still valid. A record of the consent is maintained within the officer / staff HR system; iTrent. Staff and officers will be informed that they have the right to withdraw consent at anytime,at which point their personal data will be removed from the BlueWatchlist. Should a member of staff leave the organisation, their record will be managed and removed at the LFR unit level.

	Or Article 9(2)(g) - processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;. Article 9(2)(g) requires a further schedule to lawfully meet this legal basis. Schedule 1, Part 2: Para 5 Requirement for an Appropriate Policy Document Para 6 Statutory etc, and government purposes Para 18 Safeguarding of children and of individuals at risk Furthermore, for the purposes of Part 2 of the DPA 2018, Criminal convictions and offences personal data are defined in Section 11.2 of the DPA 2018 as: *Section 11.2. …personal data relating to criminal convictions and offences or related security measures include personal data relating to—* *(a)the alleged commission of offences by the data subject, or* *(b)proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.* Processing personal data relating to criminal convictions and offences for general purposes must comply with the requirements of an Article 10.1 of the UK GDPR: *Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority* ***or*** *when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.* As GMP will only process this specific personal data type under its official authority when utilising LFR technologies for a general purpose, there are no further requirements for GMP to meet the additions requirements as laid out in Section 10(5) DPA 2018.
4.2 Is there another way to achieve the same outcome? *Can the data be anonymised or pseudonymised in any way*	No – the use of the technology is only effective if the data is gathered in the manner described.
4.3 How will you prevent function creep?	A beskpoke watchlist is created for every deployment, to ensure that the inclusion of an individual's image on a watchlist is necessary and proportionate.

i.e the gradual widening of the use of the intended purposes to which the data was originally collected/processed for.	The AO must justify which watchlists are used for any deployment. Watchlists (including biometrics) are deleted post deployment, no later than 24 hours after a deployment has finalised. Persons of interest engaged with during a deployment are to be manually removed from the database to prevent any further unnecessary processing of their personal data and to remove the risk of a further unnecessary engagement. Biometrics obtained by the CCTV footage from persons walking into the zone of recognition are deleted instantly by the system if no alert has been generated. If an alert has been generated all related personal data is deleted as soon as practicable and in any case within 31 days, except to the extent that: (i) Personal data is retained in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996; (ii) Personal data is retained in accordance with the GMP's complaints / conduct investigation policies. All CCTV footage generated from LFR Deployments is deleted within 31 days, except to the extent that the footage is retained: (i) in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996; (ii) in accordance with the GMP's complaints / conduct investigation policies; (iii) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data. By ensuring all officers / staff are adequately trained on LFR and all the accompanying policies and procedures. The generation and use of the watchlists will be reviewed on an ongoing basis to ensure that the images used for deployments remain relevant and necessary. GMP's processes surrounding the use of live facial recognition technologies will be audited by the Greater Manchester

	Combined Authority to ensure that the remit of the intended processing remains in scope.
4.4 How will you ensure data quality and data minimisation?	Watchlists will be exported as close to deployment times as possible and in any case no more than 24 hours prior to a deployment. This ensures that the software and operators are using the most current data available. The GMP LFR policy establishes conditions around image quality. The criteria for constructs of watchlists for use with LFR must be approved by the AO and be specific to an operation or to a defined policing objective. Watchlists, and any images for inclusion on a watchlist, must also be limited to the categories of image articulated in Force policy documents which are images of people who are: a. wanted by the courts; and/or b. suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or c. subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or d. missing persons deemed increased risk; and/or e. presenting a risk of harm to themselves or others. An individual's inclusion in a watchlist will be deemed strictly necessary to achieving the policing outcome and only when less intrusive means of location have proved unsuccessful. Each deployment of Live Facial Recognition will be subject to a full AO pre-deployment authorisation report which will clearly define the strictly necessary argument for processing personal data, along with setting out clearly the case for the deployment's compliance with the College of Policing's Authorised Professional Practice of being targeted, intelligence led and time bound and geographically limited. The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. The best images are those that follow a custody or passport style image that conforms to the National Policing Improvement Agency 'Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'. Images used will be as explained above at 2.1. Where multiple images of a subject are available, consideration should be given to including these in the

	Watchlist where it is advised that they will improve the likelihood of locating those of interest to GMP.
4.5 How will you help to support the data subject rights? *i.e. GMP's data being processed will be supported by GMP's Information Compliance & Record Mgt Unit.*	Information regarding GMP's LFR deployments will be made publicly available on its website, including the LFR privacy notice and appropriate policy documents to inform data subjects' rights. Any data rights requests as defined within the DPA 2018 / UK GDPR and any Freedom of Information requests should be directed to the GMP's Information Access Unit at subjectaccess@gmp.police.uk and freedomofinformation@gmp.police.uk .
4.6 Will the sharing of data involve any international transfers and how will you safeguard such transfers? *Consider if sharing data where in the world that data will be hosted/stored, i.e. UK, EU or further afield?*	It is not anticipated that any data will be transferred outside the UK as part of routine LFR activities. In rare scenarios, there might be circumstances in which it is necessary to share data with international law enforcement agencies for a strictly necessary purpose where an individual is a person of interest.

Step 5 - Identify privacy and related risks and identify measures to reduce each risk

*This DPIA assesses compliance and privacy risks for individuals, such as damage caused by inaccurate data, risk of ID theft following a security breach, or upset caused by not upholding rights or due to unnecessary privacy intrusion. Business risks should be recorded outside of this DPIA in the usual way. This assessment needs to reflect the likelihood and severity of risk **primarily for individuals** and if any residual high risks remain that cannot be reduced to an acceptable level, the ICO must be consulted. If you are uncertain how to identify or rate a risk, please seek advice from the DPO, an Information Governance lead or risk specialist.*

Risk Ref.	Description of Risk *Note: is this a risk to individuals, a compliance risk or an organisational risk?*	Likelihood, Severity and Overall risk	Solution(s)	Result – Eliminated, reduced or accepted	Measure approved?	Person responsible for risk
01	As a result of the Watchlist being deleted after 24 hours the force may be unable to comply with a subject access request from a data subject resulting in an infringement of data subject rights, complaints, reputational damage, and potential financial claims to the organisation	**Likelihood:** Possible **Severity:** Minimal **Overall Risk:** Low	The Watchlist can be re-created. This can be achieved via GMP's Records Management System 'back-end' database by recording the nominal number of an individual extracted into a Watchlist for any given date.	Eliminated	Yes /	Chief Supt – Head of FIB
02	There is a risk that intervention may take place as the result of a False Alert due to the threshold value for a similarity score being set too low resulting in individuals being stopped unnecessarily by the police. This could lead to reputational damage, potential enforcement action and financial penalties, loss of public trust and increased volumes of complaints for the organisation.	**Likelihood:** Remote **Severity:** Severe **Overall Risk:** Medium	A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithm varies dependent on demographic factors. As a result GMP has had regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST), who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by the supplier, NEC. The National Physical Laboratory (NPL) has also undertaken specific operational testing and have determined the most appropriate minimum threshold setting. For GMP, the threshold setting will ordinarily be equal to or above the value where no facial recognition system bias is detected (0.64 with the current FRT algorithm). The threshold value may be lowered based on the intelligence case	Reduced	Yes /	Chief Supt – Head of FIB

			with a full rationale detailed in the GMP LFR Application / Written Authority Document. Additionally, the LFR Operator will complete the adjudication prior to any engagement.			
03	As a result of the scope of a deployment there is a risk that fair processing information may not be widely available to members of the public resulting in them not being informed of the processing of their personal data,resulting in increased complaints, court cases, enforcement action and reputational damage.	**Likelihood:** Remote **Severity:** Significant **Overall Risk:** Medium	A communications strategy will be in place prior to any deployment to ensure that all available means of communicating the fact that a deployment will/is taking place via various channels including digital and physical, and information is available to the public on why deployments are effective to ensure that individuals and the public are confident that the decisions made to deploy and continue to operate LFR are based on firm evidence and transparent analysis. The use of cameras will also be assessed against the Surveillance Camera Commissioner's Camera Code (as required under Section 29 of the Protection of Freedoms Act 2012).	Reduced	Yes /	Chief Supt – Head of FIB
04	As a result of the nature of LFR there is a risk that deployments may limit or contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law resulting in potential legal challenge, financial claims and an increase in complaints	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** High	The assessment prior to any deployment of LFR will determine whether interference with these rights is necessary, proportionate, and lawful and whether there are less intrusive methods which could be employed. Full, robust justification will be documented prior to any deployment	Reduced	Yes /	Chief Supt – Head of FIB Delegated to Authorising Officer – Supt Rank
05	There is a risk that there may be an excessive number of images included in a watchlist for a deployment	**Likelihood:** Remote **Severity:** Significant **Overall Risk:** Medium	The assessment prior to any deployment will include the requirements and justification of the inclusion of images in the Watchlist to ensure that the strict necessity threshold is met and there is a reasonable expectation that those individuals will be in the vicinity of the deployment of LFR. Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use.	Reduced	Yes /	Chief Supt – Head of FIB (as corporate owner Delegated to Authorising Officer – Supt Rank
06	As a result of limited availability of images for testing the software there is	**Likelihood:** Probable	Assurances around the testing conducted by the software supplier are required in the contract	Reduced	Yes /	Chief Supt – Head of FIB

	a risk that bias may not eliminated in the algorithm resulting in a disproportionate number of individuals with protected characteristics being identified in False Alerts leading to potential legal challenge, financial claims and increase in complaints.	**Severity:** Severe **Overall Risk:** High	and is continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified as part of the public sector equality duty and through assessment by academic institutions, technology vendors and government opinion. Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented. Equality Impact Assessments will be completed and regularly reviewed against legal developments. The amount of personal data within the BlueWatchlist will expand over time as more staff and officers consent to their images being used for testing purposes, providing a broader spectrum of data to reduce the likelihood of bias.			
07	As a result of the wide-ranging capability of LFR to process large amounts of personal data there is a risk that the processing of personal data may be excessive resulting in regulatory action.	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** Medium	The assessments prior to a deployment will consider and document why less intrusive methods are not appropriate and justify the use of LFR based on intelligence.	Reduced	Yes /	Chief Supt – Head of FIB (as corporate owner Delegated to Authorising Officer – Supt Rank
08	There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action.	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** High	An additional legislative safeguard is any covert surveillance will require authority under the Regulation of Investigatory Powers Act 2000 as per arrangements for any covert surveillance. Furthermore, by default the vans are overt in design.	Eliminated	Yes /	Chief Supt – Head of FIB Delegated to Authorising Officer – Supt Rank
09	Due to the similarity in requirements for LFR there is a risk that each deployment and Watchlist is not subject to a full assessment documenting the rationale for inclusion of images 'the who', the scope of the location, duration 'the where' and whether the strictly necessary threshold has been met resulting in a risk of unlawful processing and breaches of the Data	**Likelihood:** Remote **Severity:** Severe **Overall Risk:** Medium	GMP LFR Policy requires a suite of documents to be completed and reviewed prior to any deployment of LFR or as soon as possible in urgent cases (e.g major incidents or terrorist attacks). These documents require authority to deploy and documents all justification, criteria and detail around necessity, effectiveness, and purpose of deployment to ensure it is targeted; intelligence led and time limited	Reduced	Yes /	Chief Supt – Head of FIB (Delegated to Authorising Officer – Supt Rank

	Protection Act 2018 which may lead to financial claims penalties, and court cases.					
10	As a result of potential incomplete deletion exercises there is a risk that Watchlists may be compiled using custody images which should have been deleted from police systems in line with established retention and deletion procedures or from images of uncertain provenance where accuracy may be an issue (e.g. sourced from social media) there is a risk that these may lead to an unjustified engagement and potentially cause unwarranted and unjustified damage and distress to individuals	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** High	Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. No engagement will be made without checks being made on possible matches without manual intervention to reduce any damage and distress.	Reduced	Yes /	Chief Supt – Head of FIB (as corporate owner Delegated to Authorising Officer – Supt Rank
11	As a result of different scenarios in which a person may be reported as missing there is a risk that the use of LFR to locate that person may not meet the strict necessity threshold and may be unlawful resulting in potential legal challenge, complaints and financial penalties or regulatory enforcement action	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** High	Where a deployment is being used to locate a missing person a strict necessity test will be conducted to determine the degree to which the missing person is vulnerable and whether there is sufficient intelligence to indicate that the individual may be in a particular area at a particular time. This will need to be signed off by an officer of the required authority.	Reduced	Yes /	Chief Supt – Head of FIB Delegated to Authorising Officer – Supt Rank
12	Where the force has not completed an appropriate policy document there is a risk that it will be in breach of Section 42 of the Data Protection Act 2018 resulting in potential regulatory enforcement action and/or financial penalties.	**Likelihood:** Remote **Severity:** Severe **Overall Risk:** Medium	The force has in place a privacy notice and 2 appropriate policy documents for LFR. One for processing under Part 2 and one for processing under Part 3 of the Data Protection Act 2018.	Eliminated	Yes	Chief Supt – Head of FIB (Delegated to Authorising Officer – Supt Rank
13	As a result of inconsistent guidance around the use of LFR there is a risk that officers may exercise too much discretion around inclusion in the Watchlists and the location of the deployment resulting in excessive and unlawful processing of data which may lead to legal challenge, complaints and potential enforcement action	**Likelihood:** Possible **Severity:** Severe **Overall Risk:** High	GMP LFR Policy stipulates documentation and authority required for a deployment ensuring consistency and oversight for each deployment, in addition to the College of Policing LFR Authorised Professional Practice and Surveillance Camera Code of Practice that must be adhered to.	Reduced	Yes /	Chief Supt – Head of FIB Delegated to Authorising Officer – Supt Rank

14	There is a risk that officers involved in the deployment of LFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the deployment of LFR and potential breaches of the DPA'18 which may result in enforcement action, legal action and financial penalties	**Likelihood:** Possible **Severity:** Significant **Overall Risk:** Medium	As part of an officer's involvement in LFR operations, appropriate training will be required on the use of the system, LFR operatives will also have completed corporate mandatory data protection training which they are required to renew on an annual basis.	Reduced	Yes /	Chief Supt – Head of FIB
15	As a result of lack of training and awareness there is a risk the data entered onto the Watchlist is not treated within the correct Government Security Classifications (GSC) system resulting in adequate protection when handled and potential loss and damage.	**Likelihood:** Remote **Severity:** Significant **Overall Risk:** Medium	GMP staff/ officers are trained in respect of the Government Security Classifications (GSC). Officers compiling Watchlists will perform this task in a secure environment to which the public do not have access. All Watchlists are appropriately stored prior to the operation and are deleted after the Deployment	Reduced	Yes /	Chief Supt – Head of FIB
16	As a result of lack of training and awareness there is a risk that the Watchlist or other data generated by the LFR application is unlawfully disclosed to third parties	**Likelihood:** Remote **Severity:** Severe **Overall Risk:** Medium	Officers/Staff compiling the Watchlists are briefed in respect of Watchlist circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff. Any action following an alert may involve GMP working with other police forces, law enforcement bodies and other agencies to assist GMP in discharging its common law policing powers. This action will not require the sharing of biometric data but may require GMP to share personal data, as it would for any investigation, in accordance with GMP's routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect the LFR application and the encrypted USBs used to import the data into the LFR application.	Reduced	Yes /	Chief Supt – Head of FIB (Delegated to Authorising Officer – Supt Rank
17	As a result of technical failure there is a risk that the equipment will not function correctly resulting in false alerts or failure to identify possible matches resulting in potential damage and	**Likelihood:** Remote **Severity:** Severe **Overall Risk:** Medium	The technology has been trialed and tested by NEC NEC algorithms have been evaluated by the National Physical Laboratory (NPL), NIST and the Department of Homeland Security.	Reduced	Yes /	Chief Supt – Head of FIB

	distress or the threat of risk and harm to others		An LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of the False Alert Rate to below 0.1% will be present at all deployments. All relevant information is logged for audit purposes. Logs are kept by the Gold, Silver and LFR Operator and LFR Engagement Officer. GMP LFR documents also outline points relating to the LFR application to ensure that it is used in a way that maximises its effectiveness. They also place responsibility on the Silver Commander and LFR Operator to continually monitor and review the system's performance. The Gold and Silver Commanders are obligated to stop the deployment, should the Deployment fail to meet the requirements of the DPA 2018 at any point. The ongoing effectiveness of GMP's use of LFR is reviewed by way of the post-deployment review process. This will help ensure that future deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.			
18	As a result of the software provider having access to the system for the purposes of providing service support if required, there is a risk that personal data may be intercepted and used by an unauthorised third party.	**Likelihood:** (Remote,) **Severity:** (, significant) **Overall Risk:** (, medium	. The provider of the Neoface software, Nippon Electric Company, will be obliged to sign a contract with GMP which will include data processing provisions setting out the parameters for their handling of personal data belonging to GMP.	, Reduced	Yes /	Chief Supt – Head of FIB (as corporate owner
19	There is a risk that the software malfunctions and biometric data and CCTV images do not autodelete where no possible match is found.	**Likelihood:** (Remote, **Severity:** (, significant **Overall Risk:** (medium	?Two members of the LFR team will receive training to become system "superusers" and will have the ability to manually delete data in the unlikely event of a system malfunction.	reduced	Yes /	Chief Supt – Head of FIB (as corporate owner

20	Loss of the encrypted USB with watchlist data	**Likelihood:** (, possible) **Severity:** (severe) **Overall Risk:** (high)	The encrypted USBs used for the transfer of watchlist data are AES-CSB 256-bit full disk hardware encryption engine devices with PIN entry activation, and is regarded as an extrenel secure means of carrying data. The transfer of data from the GMP secure network drive to the Neoface system will take place on GMP premises, thus reducing the risk of data becoming lost or corrupted as part of this process. The LFR operatives performing the data transfer will be required to maintain detailed deployment logs recording the dates and time the data is copied/transferred which includes physical transportation of the USB devices. They will be required to check the completeness of the watchlist after its initial download from the GMP network to the USB and the upload to the Neoface system to ensure that no data is lost or becomes corrupted as part of the transfer process. Officers will be required to sign the logbooks and their colleagues countersign activities recorded as an extra security measure.USBs will be stored in a secure safe box within the van once the watchlist has been downloaded.	reduced	Yes /	Chief Supt – Head of FIB (
21	Alert is actioned; engagement ensues with a positive outcome. The van remains in situ for the duration of the deployment, without the watchlist being updated. An individual already processed is re processed and re-engaged, ith an unlikely possibility of a further (now unlawful) arrest	**Likelihood:** Remote **Severity:** severe **Overall Risk:** medium	Following an initial engagement, LFR staff will remove an individual from the live watchlist. Furthermore, alerts and engagements are logged at the point of engagement. All checks are carried out by the engagement officer prior to engagement, as such if the LFR team haven't removed an individual from the watchlist following the first engagement, a second engagement is unlikely to be carried out.	Reduced	Yes /	Chief Supt – Head of FIB (Delegated to Authorising Officer – Supt Rank
22	Subject on the watchlist has been dealt with elsewhere in the Force then activates an alert walking through the	**Likelihood:** Remote, **Severity:**	Checks will be carried out by the engagement officer prior to engagement, if missed at this point and a further engagement is carried out,	Reduced	Yes /	Chief Supt – Head of FIB (

	zone of recognition,potentially leading to further engagement and a possible unlawful further arrest.	significant **Overall Risk:** medium	checks should show during the usual policing procedures that the individual has been dealt with.			
23	Additional meta data from GMP systems is used alongside the images, which is notnecessary or proportionate.	**Likelihood:** Remote, **Severity:** significant **Overall Risk:** medium	LFR staff / officers will be fully trained in the lawful and GMP procedural processes prior to being deployed. Policies and procedures are in place and are expected to be followed. The watchlist will be preset to only hold certain data sets.	Reduced	Yes /	Chief Supt – Head of FIB (Delegated to Authorising Officer – Supt Rank
24	Van is stolen; suspects can access data held within the system after the watchlist has been uploaded	**Likelihood:** Remote, **Severity:** significant **Overall Risk:** medium	Technical security measures are in place to prevent unlawful access to the watchlist and CCTV data. The LFR and CCTV systems require a username and password to gain access to the system. The Neoface server/ base unit is stored within a locked cabinet within the vehicle. The encrypted USB device, when not in active use during a deployment, is locked in a secure key safe.	Reduced	Yes /	Chief Supt – Head of FIB (as corporate owner
25	Vandalism / accidental damage of the equipment resulting in the loss of the watchlist or any positive alerts saved on the the system for 31 days	**Likelihood:** Remote, **Severity:** significant **Overall Risk:** medium	The LFR system is stand alone and is not connected to the main GMP IT infrastructure,. Thewatchlists are not stored on the LFR software while not in active use, only during deployment. At the end of the deployment the watchlist is deleted from the system. Onlythe CCTV stream is uploaded on to evidence.com so the risk of damage causing loss of data or any unauthorised access is extremely remote.			Chief Supt – Head of FIB (as corporate owner

Step 6: Sign off and record outcomes		
Item	**Name / date**	**Notes**
DPO advice provided by:	Suzanne Martin / 9th October 2025	DPO should advise on compliance, Step 5 measures and whether processing can proceed
Summary of DPO advice: I am satisfied that due diligence has been applied to the assessment of GMP's intended use of live facial recognition technology and its use is compliant with the provisions of the Data Protection Act, UK GDPR and human rights legislation. It is recognised that the technology constitutes high-risk data processing due to the involvement of biometric data and the surveillance of individuals on a large scale, but appropriate safeguards have been built into the use of the technology (outlined in this DPIA and the LFR Policy and Procedure) to ensure that the processing is proportionate for clearly defined law enforcement purposes whilst respecting individuals' privacy as far as possible. It is noted that GMP will commence its LFR deployments in the autumn of 2025 with the intention to use the technology on a permanent basis for both GMP's purposes and for the benefit of other forces, in the future, who wish to optimise the technology for their own deployments. Where GMP provides the use of its LFR vans and NeoFace software for other forces' LFR operations, GMP will become the data processor and will be acting under the instruction of that force. The force procuring GMP's services in the provision of the LFR equipment will be required to produce its own DPIA assessing the data processing risks and provide GMP with a data processing agreement (or equivalent) stipulating the parameters in which GMP is to provide the service. As the adoption of LFR technology is a new process for GMP, it is essential that the governance and execution of the processing (as documented in this DPIA) is reviewed and monitored on a regular basis, to ensure its ongoing necessity, relevancy and lawfulness. In particular, it is recommended that the process governing the creation of the watchlists is reviewed following every deployment. It is noted that the LFR system is currently hosted on a stand-alone network which is separate to the main GMP IT infrastructure, which is dependent on the transfer of data by secure, encrypted USB device. In the event that the IT hosting arrangements change in future to allow the LFR software to operate on the GMP network which would negate the requirement for USB data transfer, this DPIA will need to be reviewed to ensure that the data security arrangements remain robust. Irrespective of whether there are changes made to the delivery or governance of the LFR deployments over the coming months, it is recommended that this DPIA is reviewed at the end of the calendar year (December 2025) due to the high-risk nature of the data processing.		
This DPIA will be kept under review by:	Neil Jones.	The GMP SPOC is responsible for reviewing this DPIA should there be any future changes. Any review/changes should be completed in consultation with the DPO