Classification	OFFICIAL
Handling Instructions	No restriction on distribution
Disclosable (FOI / Publication Scheme)	Yes

Data Protection Impact Assessment (DPIA) – Stage 2	
Project Name	Live Facial Recognition
Project Lead	LFR Business Lead
Division/Department	B Division
Information Asset Owner	C/Supt Chris Casey
Date for start of intended processing	December 2025
Date submitted to Information Management	10/02/2026

A DPIA is a Data Protection risk assessment which must be considered and completed if required before commencement of any project or initiative involving the processing of personal data. Therefore, the process should be started during the early planning stages of any project and have received approval from the Force Data Protection Officer before any data is processed.

The DPIA processes helps the organisation to identify and fix any problems at an early stage in a project and therefore helps to avoid later data breaches or non-compliance with Data Protection requirements that can otherwise be the subject of significant financial penalties. The process assists BTP in complying with our obligations to process personal data in a lawful, fair and transparent manner and to be accountable for how we do so.

This 'stage 2' form should only be completed on instruction of Information Management following assessment of a Stage 1 DPIA form.

Information Management Outcome (IM Use Only)	
Residual risks have been mitigated to acceptable levels – signed off by Force DPO	☐
Medium to high risks remaining to be accepted by Force – escalated to Force SIRO	☐
High residual risk that cannot be mitigated – referral to ICO required	☐
Approved By	
Role	
Date	

Responsibility for Mitigation Factors	
The risk assessment completed has been signed off based on the delivery of the mitigations detailed in Sections 3 and 4.	
Actions Assigned To	
Expected Completion Date	
Actual Completion Date	
Sign Off Completion (IM use)	
Review Date	

Section 1: Stage 1 Assessment

This form is the second part of a two-part assessment and should only be completed when advised by Information Management following submission and return of a Stage 1 assessment. Please embed a copy of the completed Stage 1 assessment returned by IM below.

Section 2: Compliance with Data Protection Principles

In this section you will set out how the project/initiative will comply with each of the 'Data Protection Principles' which are set out at Article 5 of UK GDPR (for general processing) and Part 3, Chapter 2 of the Data Protection Act 2018 (for law enforcement processing) as well as how you will ensure that we can comply with the various rights that data subjects have over their data.

2.1 Principle 1: 'Lawfulness, fairness and transparency'
How will data subjects be aware of the processing? Do you need to create or amend an existing Privacy Notice?

Personal data must be processed through an LFR deployment in accordance with our policing purpose; either for a law enforcement purpose, or for general processing purposes (e.g: missing persons, vulnerable persons). ***At commencement of LFR pilot (Feb 2026) missing people will not be included in watchlists until further DPIA and EIA consideration is concluded***

In reaching this conclusion BTP has considered the (i) the legal position and legislative context (ii) the use cases for LFR and how they fit in a law enforcement context and (iii) the rights and freedoms of data subjects, including any impact on such subjects from processing data under Part 3 of DPA 2018 and also Part 2 DPA 2018 (UK GDPR) processing.

To process data under Part 3 of DPA 2018, the processing needs to fall within a law enforcement purpose. This term is defined at Section 31 and means: '*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.*'

Before determining that a LFR deployment meets the strict-necessity threshold, BTP must assess whether the policing objective could be achieved through less intrusive means. The following alternatives should be considered

1. Increased officer presence
2. Retrospective facial recognition only
3. Manual CCTV review
4. Use of intelligence-led patrols alone
5. Use of non-biometric analytics

Conclusion:
Where each alternative has been assessed and determined to be insufficient to meet the policing objective, LFR may be therefore deemed strictly necessary because it is the least intrusive measure capable of reliably identifying sought persons in real time within the intended operational environment.

This satisfies the requirement for documenting less-intrusive means prior to asserting strict necessity.

Where BTP 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 conditions

The use cases outlined at section 3 of BTP's LFR Policy will ensure that the BTP is acting with a law enforcement purpose when it deploys LFR.

It should be recognised that 'Consent' is impractical in the context of LFR. Accordingly where sensitive processing is undertaken for a law enforcement purpose, in line with Section 35(5)(a), one of the conditions set out at Schedule 8 of the DPA 2018 will need to apply. The relevant condition is likely to be one of:

1 Statutory etc purposes
2 Administration of justice
3 Vital Interests
4 Safeguarding of children and of individuals at risk
Appropriate Policy Document

Section 42 of the DPA requires that, at the time the processing is carried out, an 'appropriate policy document' is in place. This document can be found on the BTP website at the following link:

Facial Recognition Technology | British Transport Police

Part 2 Data Protection Act 2018 / UK GDPR "General Processing"

UK GDPR - For General Purpose: Where BTP 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:

- 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 as relevant:

- Article 9(1)(a) – *the data subject has given explicit consent to the processing for one or more specified purposes.*

- Article 9(1)(g) – *processing is necessary for reasons of substantial public interest*

Where article 9(1)(g) is relied on, Section 10 of the DPA 2018 supplements this and requires one of the following conditions of Schedule 1 to be satisfied:

Part 1:

- Statutory etc and research government purposes
- Safeguarding of children or individuals at risk

Part 2

- Statutory and government purposes
- Safeguarding of children

In terms of LFR operators and BTP officers participating in the BlueWatchlist testing, such processing will be conducted in accordance with Article 6(1)(e) Public Task. Participants in blue watchlist testing will agree to take part which is recorded and managed to ensure the facilitation of individual rights, including requests for deletion of data. Should a member of staff leave the organisation, their record will be managed and removed.

At commencement of LFR pilot (Feb 2026) missing people will not be included in watchlists until further DPIA and EIA consideration is concluded

Appropriate Policy Document

Processing under UK GDPR of special category data in line with the conditions at Schedule 1 of the DPA 2018 requires that, at the time the processing is carried out, an 'appropriate policy document' is in place. This document can be found on the BTP website at the following link:

Facial Recognition Technology | British Transport Police

Fairness

The following section will address the fairness of LFR deployments conducted by BTP, balancing the rights and freedoms of data subjects against utilising LFR for a law enforcement purpose. This will include how personal data is being processed during an LFR deployment, how a deployment is conducted and how we intend to mitigate risks around disproportionality in terms of use and processing.

Any deployment will capture images of individuals passing through the zone of recognition. LFR technology will create biometric profiles of individuals within the zone of perception and as such data subjects have reasonable and understandable grounds to expect that any biometric data created about themselves will be handled appropriately and disregarded if no match is found.

Similarly data subjects whose data is included on a watchlist will have an expectation that their data is only used strictly for policing purposes. The inclusion of this data into a watchlist would need to be deemed necessary and proportionate in order for BTP to achieve its policing aims in the prevention and detection of crime, protection of life and property. The personal data should not be included in a speculative manner, and without a duly considered and approved justification case. This will also extend towards any use of images that have been sourced from third parties (including other Home Office Police Forces) that are subjected to LFR might be used by BTP for a separate purpose to which the originating party obtained the image.

Automated processing - LFR will use an algorithm which should not be treated as an entirely automated tool; there should always be manual, human led judgement throughout a deployment. An alert from the LFR system alone is not enough to justify arrest, search or detention. A BTP officer must always be involved to assess the situation and decide on the most appropriate response. This decision will be based on the information available at the time and officer's interaction with the individual identified by the system.

BTP will not deploy LFR as a standalone operation but alongside existing operations as a tactical option to enhance organisational effectiveness.

Addressing Disproportionality - The risk of bias or of targeting specific demographics arising through use of LFR would have a serious effect in undermining the lawful basis for deployments undermine the confidence of the public in terms of our ability to deploy LFR in a fair and proportionate manner.

To that end BTP does not create or retain a breakdown of race, gender or any other protected characteristic of persons on a watchlist. The deployment of LFR will be driven by BTP policing priorities, and also intelligence-led assessment, both of which determine locality and the policing purpose. BTP are creating dashboard for LFR (still under construction) that will give us some visibility on ethnicity composition of our watchlist but this is only for the purpose of monitoring for disproportionality and understanding of potential total numbers of persons on a watchlist.

The locality and policing purpose determines the composition of the watchlist. The individuals are included on a watchlist because there is a policing need to locate them, there are realistic prospects of doing so, and that need fits with the policing purpose driving the LFR deployment on that specific date and time.

The routine retention of data relating to protected characteristics would mean BTP holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a watchlist.

BTP does however recognise the duty placed on us as a public authority under the Public Sector Equality Duty (Equality Act 2010) to consider the impact of universal and situational protected characteristics and to eliminate discrimination and advance equality of opportunity. BTP's Equality Impact Assessment for LFR will explore how BTP will seek to mitigate any undue consequences through its use.

Bias

BTP recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and that in this context they do not disadvantage individuals based upon protected characteristics. Regular tests will be carried out using police officers and staff volunteers who are 'seeded' into a 'Blue Watchlist'. The volunteers will walk through the Zone of Recognition at the start of a deployment to measure the number of times those subjects are present in the Zone of Recognition against the number of alerts generated.

BTP has a number of measures to guard against a System Factor (system bias) affecting the generation of alerts. For example, being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:

- Those involved in an LFR deployment monitor alerts, subject factors, system factors and environmental factors throughout the deployment. Should concerns arise that the LFR system is not performing correctly, the Sliver Commander will halt the deployment where necessary, and
- For the purpose of facilitating post-deployment reviews, alerts are retained for up to 24 hours. It provides further opportunity to consider the subject, system and environmental factors, alert reliability, and the effectiveness of the safeguards in place for the deployment, including the reviews undertaken by Silver and Gold during the deployment, and
- In the event post-deployment reviews identify an area of concern, BTP may approach the supplier to undertake further equitability testing where this appears necessary.
- The 'similarity score threshold setting of 0.64. This threshold is chosen to balance **accuracy and bias mitigation**—lower thresholds may increase false positives, while higher thresholds may reduce bias and improve fairness.

The supplier for the LFR have submitted their algorithm to the National Physical Laboratory for testing of accuracy and equitability. The National Physical Laboratory provide the main independent test used by UK Police Forces. The results are available to BTP for scrutiny.

Here is a link to their webpage:
Operational Testing of Facial Recognition Technology

Here is a direct link to the report:
frt-equitability-study_mar2023.pdf

Transparency

Overt LFR deployments will be conducted in a transparent manner. During a deployment BTP will ensure that awareness raising measures will be in place to ensure that the policing presences is clearly overt and as such the public in the vicinity of and passing through the zone of recognition can recognise and understand that LFR is being used at the location and understand the nature of the data that will be processed through the deployment. The placement of the camera equipment will be overt, highly visible and obvious as a 'police' deployment distinct from standard fixed CCTV that passengers would expect to already be present on the railway network.

This will include notices with a brief explanation and reference to the BTP LFR webpage are displayed immediately before the operational area. LFR cameras will be deployed on at the required location (a highly visible mobile camera column) along with appropriate signage and officers on scene. Information can be offered to persons at the location verbally, in writing or via QR codes displayed on signage. During deployments, announcements will be made over station Tannoy systems where appropriate for the station layout and size. (The LFR EIA notes the use of public announcement systems as a way of informing vulnerable communities, such as the blind, of LFR deployments is possible but this will need to be managed on a location by location basis to ensure Tanoy announcement don't confuse or give rise to the apprehension that the entire station is under LFR surveillance)

Social media and other external communication channels will be utilised to highlight to the public in advance that BTP will be conducting an LFR deployment. Deployment locations will be carefully considered before any deployment is undertaken to ensure that station users are not forced to enter the zone of recognition and that there are clearly signposted alternative routes that may be used to avoid the zone of recognition without any detriment or inconvenience.

The pre-deployment assessments will consider and address any specific requirements likely to be encountered by virtue of the location where the deployment is being conducted. An Equality Impact Assessment has been conducted in relation to deployment of LFR technology and is available on the BTP website.

Following any deployment the outcome of and results of LFR deployments are subject to evaluation and will be posted on the BTP website for the public to access the appropriate levels of information regarding the results. Details of the report will include the location, date and duration of deployment, number of subjects included on the watchlist, the minimum threshold setting, total number of alerts and the number of confirmed true alerts and confirmed false alerts, the number of unconfirmed true alerts and false alerts, the false alert rate, and estimated number of faces scanned during the deployment. No personal data will be published as part of the report, however the post-deployment process will include a report of the breakdown of demographics.

BTP have a privacy notice for members of the public published on our website:
https://www.btp.police.uk/hyg/btp/privacy-notice/

2.2 Principle 2: 'Purpose limitation'
How does the processing achieve the purpose? Will the data be used for any other purpose? How will you prevent scope creep?

LFR helps BTP to locate those on a watchlist by monitoring facial images of people within a zone of recognition. Images from cameras attached to the LFR system are searched against a watchlist of images of people who are wanted or are suspected of posing a risk of harm to themselves or others. The watchlist composition will normally be restricted to individuals suspected to be in the proximity of the deployment area and where there is some possibility or likelihood of an individual passing through the deployment zone whilst recognising the transient nature of criminal movements through railway transport hubs. Those 'sought' persons on a British Transport Police 'watchlist' have either already demonstrated offending on the rail network and use of train services, stations or rail infrastructure to facilitate that offending, or BTP will have established that individuals pose a significant risk to themselves e.g. vulnerable persons, missing person) ***At commencement of LFR pilot (Feb 2026) missing people will not be included in watchlists until further DPIA and EIA consideration is concluded***

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. Deployment record - 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 bespoke watchlist will be created twenty-four hours ahead of each deployment, to ensure that the inclusion of an individual's image on a watchlist is necessary and proportionate. 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. Therefore this data will not be retained in which case any potential alternative use of this information is not possible.

Scope creep will also be mitigated by ensuring all officers / staff have received appropriate training on the LFR system and all the accompanying policies and procedures. The supplier will initially provide a level of training to the proposed operators in the lead up to the initial planned deployment.

A potential risk of scope creep could arise from use of images provided by a third party that were originally obtained for a different purpose. In consideration of this we will only use custody images with the recent addition (result of consultation) of the below.

In exceptional circumstances where there is an imminent and credible threat to public safety, a CCTV image of an unidentified suspect may be included on the Live Facial Recognition (LFR) watchlist. This inclusion must be authorised by the Gold Commander for the LFR operation and supported by a documented assessment demonstrating that the use of the image is lawful, necessary, and proportionate to prevent serious harm. The decision must consider the expected level of privacy intrusion (rated on a scale of 1–5 as outlined in Appendix G of the Policy) and include a clear justification of the imminence of the threat and why alternative measures are insufficient.

2.3 Principle 3: 'Data minimisation'
Is the data processed limited to only what us required for the purpose? Why do you need to use personal data at all, and why is all of the data included necessary? How do you limit access/use of the data only to people who need to do so?

Data included in the watchlist will be benchmarked against NPCC watchlist composition advice. In terms of reducing the amount of personal data (or anonymising/depersonalising the data) is simply not possible as the technology will not be effective if the data is used in this way.

Excessively minimising the amount of data held on a watchlist may present risks – for example if an LFR deployment lacked the appropriate level of data required for the planned processing, then there is a risk that the objectives will not be achieved. For those on an LFR Watchlist this may risk engagements between them and the Police taking place unnecessarily, whereas adequate data would have led to a different outcome – e.g. for those passing through the Zone of recognition, inadequate data could result in higher levels False Alerts. For those subject to False Alerts, inadequate data would risk more lengthy engagements with BTP to establish the correct position.

- Section 9.4 of the Policy sets out the criteria for the types of images that may be included on a watchlist and the intelligence case required to underpin inclusion.
- Section 9.1 and 9.2 of the Policy sets out the requirements for image quality, ensuring that images are of sufficient quality
- Section 12 of the Policy sets out the key performance metrics that will be collected and published following each LFR deployment.

Similarly, processing excessive data (i.e. too many images included on the watchlist) within the planned deployment presents risks. The necessity and proportionality argument becomes less strong, and therefore the likelihood of the public losing confidence in BTP's ability to utilise LFR in a fair and proportionate manner.

- Section 9.4 of the Policy sets out the criteria for the types of images that may be included on a watchlist and the intelligence case required to underpin inclusion.
- Section 9.9 of the Policy addresses potential disproportionality in the data collated or retained in relation to a watchlist.
- Sections 3.5 and 3.6 of the Policy set out the specific use cases of LFR and the authorisation process which will ensure that processing is proportionate.
- Section 4.4 of the Policy sets out the proportionality and Human Rights considerations that will be undertaken by the Authorising Officer before authorisation of a deployment.

If individuals are added to a watchlist as 'sought persons' when they have already been located by other means, this could lead to unnecessary engagements.

- Section 9.5.3 sets out that a watchlist will be created no longer than 24 hours before deployment ensuring that the list is as accurate and up to date as policy.

For the purposes of the pilot images taken from CCTV and Bodyworn video will not standardly be used in the watchlist images – only in exceptional circumstances would a CCTV probe image be considered for inclusion.

- Section 9.2.1 of the Policy sets out the circumstances and authorisation process for inclusion of a probe image that doesn't derive from a custody image.

2.4 Principle 4: 'Accuracy'

How will you ensure data quality? What is the process for correcting or amending any inaccurate data? Who is responsible to ensuring all the data is accurate?

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 criteria for constructing watchlists for LFR use 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 ***At commencement of LFR pilot (Feb 2026) missing people will not be included in watchlists until further DPIA and EIA consideration is concluded***
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. *Please note that subjects in category (d) will not be included in the pilot.*

Each deployment of Live Facial Recognition will be subject to a 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 APP 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)'. To comply with this BTP will be using images from our Niche system for the purposes of the LFR pilot. We would only utilise PND for when BTP don't hold a custody image. Additional checks to ensure the custody image held on PND is lawfully held will be implemented but where that confidence cannot be gained, the nominal will not be added to the watchlist.

Algorithm accuracy:

The accepted accuracy measure that will be adopted by BTP is the 0.64 confidence rating (Face-Match Similarity Threshold) which has been independently tested to provide no ethnicity bias in any alerts by the system. Cameras are rated to 30 frames per second.

2.5 Principle 5: 'Storage limitation'
Is the processing included on an existing record retention schedule, or will a new one need to be created? Who is responsible for weeding records? Can data be permanently deleted from any systems used?

BTP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the BTP LFR Policy. This means that:

- Where the LFR system does not generate an alert, that a person's biometric data is immediately deleted by the LFR software.
- The LFR watchlist is deleted as soon as reasonably practicable, and in any case within 24 hours, following the conclusion of the deployment.

Where the LFR system generates an alert, all related personal data is deleted as soon as practicable and in any case no longer than 24 hours post deployment, except to the extent that:

Where the LFR system does not generate an alert, all related personal data is immediately destroyed.

All CCTV footage data (non-biometric) generated from deployments will be retained as per below:

- CCTV footage from the camera mast will be deleted every 31 days (automatically records over unless we require it for a complaint or separate criminal investigation (such as one of our officers being assaulted whilst on an LFR operation).

- In accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996.
- In accordance with BTP's complaints/conduct investigation policies.
- 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 Closed Circuit Television (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.

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

Following each LFR deployment debrief, and review shall be conducted, to ensure future deployments reflect learning identified from each deployment, and that the use of LFR remains an effective and proportionate policing tool. This debrief should be conducted as soon as reasonably practicable but no later than 31 days after a deployment.

Post deployment an entry on the register of deployments is required to be completed. Any deployment of LFR must be recorded on a centrally held register by the LFR Operator. This register will record:

- Name and rank of the AO and Command Teams
- Date, time duration and locality of the deployment
- Watchlist composition statistics (not including any personal data) and the number of alerts, broken down as true alerts and false alerts BTP is committed to ensuring that all required LFR documentation is regularly reviewed and updated in accordance with the law and LFR landscape.

2.6 Principle 6: 'Integrity and Confidentiality'

What measures are in place to prevent unauthorised or accidental access, loss or corruption of data? What training/guidance is given to staff? How will you identify and manage a breach? How

will systems be tested? If we are using an external provider, how will we assure their processes, systems, staff and premises?

The NeoFace LFR system will operate on a standalone server on a laptop located at the site for deployments. The computer hosting the LFR system will not be connected to the main BTP network. The Watchlists including images will be stored on an isolated BTP 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. The download of the watchlist to the USB device will take place on BTP premises and not at the LFR deployment site.

The watchlist will be uploaded to the standalone laptop at location once system tests have been completed. 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 BTP network to the LFR system. Access to the USB device containing the Watchlist is limited to those with a need to use it, who have completed BTP's LFR training. Engineers will be required to delete files from laptop and server on the completion of the operation - this will be documented in the operational log as the final entry. Any alteration to the watchlist during the deployment must be recorded in the operational log and approved by the Bronze commander.

The USB stick which contains the watchlist will remain on the operators possession at all times during the operation. Operators will work in order of preference 1) A secured vehicle, 2) A private secured office, 3) On concourse with privacy filter on laptops and a medical style privacy screen around the working area to shield any data from public view. The watchlist is added to the server secured inside the lockable compartment of the actual LFR mast & cameras. This camera and mast will always be monitored with officers in close proximity.

The loss or theft of any LFR hardware (laptop, mobile device, camera, etc.) or other data, irrespective of whether protected by encryption, must be reported immediately to the AO/Gold, Silver and BTP's Data Protection Officer and Senior Duty Officer for immediate risk treatment and early recovery exploration. The control room should be notified and a log created due to the capability of the asset. Force policy on lost / stolen items should be followed at all times.

BTP have confirmed with the supplier that although they provide the technology and hardware, the supplier is not a data processor in this instance. They have confirmed that they have no access to the system remotely and it is entirely contained within the mobile camera column no transmission to elsewhere (other than the laptop and handsets owned by BTP), it is entirely standalone.

Governing the Watchlist

The systems used to generate the watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.

BTP LFR documents provide measures to ensure that the watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

The watchlist for any BTP deployment will be created no longer than 24 hours before a deployment and is required to be reviewed and approved by BTP's Head of Intelligence or a suitable nominated deputy before any deployment can take place.

The inclusion of Sought Persons on any particular watchlist is responsive to the particular use case being considered for LFR deployment and subject to the availability of watchlist images.

2.7 Data Subject Rights

How will you recognise any data subject rights requests and ensure they are passed on to Information Management? If a data subject wants to exercise their rights over data relating to them how will you be able to comply with such a request? Consider how a copy of the data can be provided, amended, restricted or deleted.

British Transport Police have a dedicated team for responding to data subject rights requests and are able to retrieve images from specific systems being used. Any requests can be forwarded to DataProtection@btp.police.uk

Section 3: Risk Assessment

In this section you will identify all data protection risks posed by the project. You will need to consider the impact of the risks along with any harm or damage that may be caused to both the individual and the organisation.
Risks may occur at various stages throughout the project, so please consider the project as a whole, rather than only risk's identifiable at the start of the project.

Where risks are identified, steps must be taken to eradicate or mitigate the risk.

Examples of risks to individuals and possible mitigations are listed below.

Risk to Individual	*Consequent Risk to Organisation*	*Examples of Possible Mitigations*
• *Discrimination* • *Identity theft* • *Financial loss* • *Reputational damage or embarrassment*	• *Failure to protect the public* • *Loss of public confidence* • *Civil litigation* • *Reputational damage*	• *Deciding not to collect certain types of data* • *Reducing the scope of processing*

• *Physical harm* • *Wrongful arrest or prosecution* • *Loss of confidentiality* • *Inability to exercise rights*	• *Regulatory action* • *Breaching other legal obligations* • *Decrease in data quality*	• *Reducing retention periods* • *Taking additional technical security measures* • *Following approved codes of conduct* • *Restricting access to data* • *Training staff to understand the risks* • *Anonymising or pseudonymising the data* • *Using different technology* • *Using an alternative third party processor*

Risks will be evaluated using the criteria below.

Severe	**Medium risk**	**High risk**	**High risk**
Significant	**Low risk**	**Medium risk**	**High risk**
Minimal	**Low risk**	**Low risk**	**Medium risk**
	Remote	**Possible**	**Likely**

3.1 Risks Identified in Section 2 (Compliance with Data Protection Principles)
List below any risks which were identified in the completion of section 2.

Please describe the risk including the source and the potential risks to individuals.	**Likelihood of harm**	**Severity of harm**	**Pre mitigation Risk rating; *High (5-6) Medium (4) Low (2-3)***	**Mitigation**
Processing data in a way that is unfair, that is, it is unwarranted or otherwise excessively interferes with the privacy rights of affected individuals, taking into account their reasonable expectations and the wider circumstances of the particular case	2 - Possible	3 - Severe	High	Full pre-deployment assessment to be conducted by Authorising Officer and approved before any deployment takes place, taking into consideration the case use, watchlist composition, location and any mitigating circumstances. The LFR system will be conducted in an overt manner. All processing to follow the LFR policy drawn up by BTP.

				Transparency through appropriate signage, comms LFR deployments to be conducted in an overt manner with deployment taking place in accordance with all relevant APP guidance.
For data subjects on an LFR Watchlist and those passing through the Zone of Recognition, if the deployment of LFR is more impactful on those with a particular Protected Characteristic, there is a risk that the Deployment would be unfair.	2 - Possible	3 - Severe	High	Pre-deployment site assessments and deployment design will ensure that subjects can follow a clearly signposted and equally accessible alternative route to avoid the zone of recognition without detriment or inconvenience. An equality impact assessment has been undertaken and published on the BTP website to ensure that there is no disproportionate detriment. The authorising officer will consider before authorising a deployment any consequences of the location, date or timing of a deployment that could disproportionately affect a group or individuals. LFR system will be monitored throughout the deployment, in particular false alert rate. Algorithm has been subject to the relevant testing and uses the 0.64 confidence rating (Face-Match Similarity Threshold) which has been independently tested and is above the threshold recommended

Processing Watchlist images for additional purposes in order to deploy on LFR, including those provided to the BTP by third parties. The BTP's law enforcement purpose may differ to the original purpose for which the third party held the image. This may fall outside the reasonable expectation of privacy and therefore intrusion and impact may be higher on data subjects as a result.	2 - Possible	3 - Severe	High	CCTV probe images would only be being used on a watchlist for LFR deployment in exceptional circumstances during the pilot. We haven't developed a process yet for accepting or verifying external forces requests to include someone on a BTP watchlist.
Using LFR for a different purpose; Acting outside of the defined case use or changing use case following authorisation would fall outside the public's expectation of privacy and would risk a significant chilling effect. A failure to mitigate this risk could also result in unlawful detention of those on the LFR Watchlist.	2 - Possible	3 - Severe	High	Policy outlines the permissible case uses for LFR, should the case use for a deployment differ than from the policy then authorisation would need to be required before proceeding and if necessary DPIA to be revisited.
Insufficient data processing: If an LFR Deployment lacks the minimum level or quality of data needed for the planned processing, there is a risk that the objectives will not be achieved, and inadequate data could result in higher levels False Alerts. For those subject to False Alerts, inadequate data would risk more lengthy Engagements to establish the correct position.	2 - Possible	3 - Severe	High	Policy establishes the image quality to be used. Timely creation of watchlist within the timeframe specified in policy Policy makes clear the specific criteria for watchlist selection Ongoing review during the deployment Post implementation review to be conducted.
Excessive data processing; the data processed needs to be proportionate to the deployment of LFR. Particularly for those	2 - Possible	3 - Severe	High	Refer to policy – which outlines the only use cases permissible for LFR, and Watchlist to be appropriate

passing through the Zone of Recognition, if the data is not really needed (i.e. not all cameras are needed) and could be removed from the use of LFR without undermining its delivery, there is a danger of unjustified collateral intrusion.				in response to the use case. Pre-deployment site assessments and deployment design will ensure that subjects can follow a clearly signposted and equally accessible alternative route to avoid the zone of recognition without detriment or inconvenience. System design – LFR systems should undertake checks to flag images of poor quality Manual adjudication from LFR operators in real time, in particular ongoing review of True/False alerts. Deletion of images from the watchlist during deployment to prevent multiple/excessive engagements in response to irrelevant data. Post-deployment review will be conducted to flag data issues. 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.
Irrelevant data processing; if LFR uses more data than it needs to achieve its aim, this would intrude into people's private lives where there wasn't a need to do so and it risks undermining trust and confidence in BTP. • if the image quality is not sufficient to generate True Alerts, such data risks increased False Alerts and unwarranted Engagements with data subjects; • if Sought Persons are added to the Watchlist where the matter has been resolved by other means, this risks unwarranted engagements as a result of irrelevant data being processed.	2 - Possible	3 - Severe	High	Refer to policy – which outlines the only use cases permissible for LFR, and Watchlist to be appropriate in response to the use case. System design – LFR systems should undertake checks to flag images of poor quality Manual adjudication from LFR operators in real time, in particular ongoing review of True/False alerts. Deletion of images from the watchlist during deployment to prevent multiple/excessive engagements in response to irrelevant data. Post-deployment review will be conducted to flag data issues.
Inaccuracies in the data itself; the data should be accurate, and where necessary, kept up to date with systems in place to erase or correct errors as needed. Inaccuracies in the data risk those added to an LFR Watchlist being subject to unwarranted Alerts/Engagements and could result in unlawful detention.	2 - Possible	3 - Severe	High	Timely creation and importing of watchlist data into the LFR system to ensure the most current data is available. If necessary review PNC and other systems prior to creation of the watchlist (and during deployment) to avoid any individuals subject to warrants that have expired. Only images of the appropriate quality are to be imported into the system to reduce risk of inaccuracies.

				Human review of the alerts flagged by the system.
Inaccuracies in the algorithm – if the algorithm is inaccurate then this may adversely impact on the data subject in a number of ways including; Unnecessary data processing where the algorithm could be assessed upfront to be an unviable proposition to policing; Potential impact on individuals passing through the zone of recognition especially in the context of false alerts; A failure to achieve the objectives for LFR such that data is needlessly being processed if the LFR system is not able to reliably generate true alerts.	2 - Possible	3 - Severe	High	Testing will have been undertaken with the supplier and will continue to be scrutinised throughout deployment and as part of post-deployment review. Algorithm confidence threshold is set at 0.64
As a result of limited availability of images for testing the software there is 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.	Possible	Severe	High	Assurances around the testing conducted by the software supplier are required 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
Data Retention; there is a risk that if the retention periods in the Policy are not applied and the data is not subject to meaningful review, it is retained where there is no need to do so.	Possible	Severe	High	BTP has established and published retention periods – data is processed in accordance with Part 3 of the Data Protection Act 2018. SD cards will overwrite every 31 days automatically, so there are in-built mechanisms for deletion. Audit logs of the deployment are retained.
Data Security; People's privacy and wider interests can be put at risk if their personal data is not protected by adequate technical and security measures from both internal and external risks. This would have a sever impact on the individual should it fall into the wrong hands	Possible	Severe	High	Access to the watchlist will be restricted to the Authorising Officer, LFR operators and prior to deployment FIB staff with responsibility for assisting in collating the watchlist. LFR operators will be fully trained and vetted to the appropriate level. At deployment locations, physical security measures will be in place to ensure that LFR equipment is secure and the working area is in a separate room or protected by appropriate privacy screens to ensure confidentiality of data. The LFR system includes a number of physical and technical security measures which are set out at Section 6.6 of the Policy.

				Supplier will not have access to any of the footage, watchlist data or matches data.
Data Loss; If data is not accessible or otherwise corrupted (through unlawful action or accident) it may undermine the ability to deploy LFR. It may also prevent the BTP acting on, and reporting on the results of an LFR deployment.	Possible	Severe	High	Reporting processes are in place as per Section 6.5 of the Force Policy. Security measures will be in place around the devices when being used The LFR deployment will be resourced at all times whilst deployed. They will be positioned under existing CCTV covered areas of the station and a physical barrier placed around the camera mast and battery storage.
Data Subject Rights requests; 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	2 - Possible	2 - Significant	Medium	Dedicated BTP team for dealing with any data subject rights requests received. Officers deployed to LFR operations will be briefed on the process to ensure that data about a data subject is extracted and retained securely in the event that a data subject makes a verbal request at the scene. Departments who may receive a written request which constitutes a data subject rights request (including the data protection team, First Contact Centre and Professional Standards Department) will be briefed on how to pass the requirement to preserve data to the LFR team.

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.	2 - Possible	2 - Significant	Medium	Threshold is set at 0.64 confidence.
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.	2 – Possible	3 – Severe	High	Each deployment subject to the pre-implementation authorisation to ensure that forward communications are proportionate and appropriate for the deployment, and that all relevant signage is in place at the deployment site. A comms plan is in place with partners.
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.	2 - Possible	3 - Severe	High	This project and policy is only concerned with overt use of LFR. Any covert surveillance would require authority under the Regulation of Investigatory Powers Act 2000 as per arrangements for any covert surveillance.
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	2 – Possible	3 - Severe	High	Source of images limited to policing systems Watchlists will be limited to accurate, verifiable images lawfully held by the Police for a law enforcement purpose at the time of use.

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				Engagement should not take place without manual checks taking place on possible matches in order to reduce any damage or distress.
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	2 - Possible	3 - Severe	High	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.
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.	2 - Possible	2 - Significant	Medium	Officers are trained in respect of the GSC. Officers compiling watchlists will perform this task in a secure environment where the public cannot access, and all watchlists are appropriately stored prior to the operation and are deleted after the deployment.
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	2 - Possible	2 - Significant	Medium	As part of an officer's involvement in LFR operations, appropriate training will be required on the use of the system.

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	2 - Possible	3 - Severe	High	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. It is not anticipated that BTP will share watchlists outside of the organisation. Physical and technical safeguards will be enforced at all times to protect the LFR system and the watchlists.

Section 4: Law Enforcement Processing Requirements

This section only needs to be completed if you identified in Stage One, Section 2.1 that data was being processed for a law enforcement purpose. Law Enforcement processing imposes additional requirements under Part 3 of the Data Protection Act.

4.1 Data Logging (Section 62, Data Protection Act 2018)

When law enforcement data is processed electronically it is mandatory to keep logs of specific actions. Please confirm whether any systems used for processing will keep a log of all the following actions on the data processed:

Collection; Alteration; Consultation; Disclosure; Combination; Erasure.

If you select 'no' please record as a risk below.

Yes

Please describe the risk including the source and the potential risks to individuals.	**Likelihood of harm**	**Severity of harm**	**Pre mitigation Risk rating; *High (5-6) Medium (4) Low (2-3)***	**Mitigation**
	Select	Select	Select	

4.2 Categorisation of Data Subjects (Section 38, Data Protection Act 2018)

Law enforcement processing requires that there must be a clear distinction between different categories of data subjects. Please confirm whether records/systems used will clearly distinguish between data subjects in the following categories?

Suspect of Criminal Offence; Convicted of Criminal Offence; Victim of Criminal Offence; Witness to Criminal Offence.

If you select 'no' please record as a risk below.				
Yes				
Please describe the risk including the source and the potential risks to individuals.	**Likelihood of harm**	**Severity of harm**	**Pre mitigation Risk rating; *High (5-6) Medium (4) Low (2-3)***	**Mitigation**
	Select	Select	Select	

Section 5: Residual Risk

All risks identified in sections 3 and 4 should be shown below and a rating assigned for residual risk after mitigations have been applied.

Risk Summary	**Pre mitigation Risk rating; *High (5-6) Medium (4) Low (2-3)***	**Result of Mitigation**	**Post mitigation Risk rating; *High (5-6) Medium (4) Low (2-3)***
Processing data in a way that is unfair, that is, it is unwarranted or otherwise excessively interferes with the privacy rights of affected individuals, taking into account their reasonable expectations and the wider circumstances of the particular case	High	Likelihood of risk reduced due to mitigations	Medium
For data subjects on an LFR Watchlist and those passing through the Zone of Recognition, if the deployment of LFR is more impactful on those with a particular Protected Characteristic, there is a risk that the Deployment would be unfair.	High	Likelihood of risk reduced due to mitigations	Medium
Processing Watchlist images for additional purposes in order to Deploy LFR, including those provided to the BTP by third parties. The BTP's law enforcement purpose may differ to the original purpose for which the third party held the	High	Likelihood of risk reduced due to mitigations	Medium

image. This may fall outside the reasonable expectation of privacy and therefore intrusion and impact may be higher on data subjects as a result.			
Using LFR for a different purpose; Acting outside of or changing use case following authorisation would fall outside the public's expectation of privacy and would risk a significant chilling effect. A failure to mitigate this risk could also result in unlawful detention of those on the LFR Watchlist.	High	Likelihood of risk reduced due to mitigations	Medium
Insufficient data processing: If an LFR Deployment lacks the minimum level or quality of data needed for the planned processing, there is a risk that the objectives will not be achieved. For those passing through the Zone of recognition, inadequate data could result in higher levels False Alerts. For those subject to False Alerts, inadequate data would risk more lengthy Engagements to establish the correct position.	High	Likelihood of risk reduced due to mitigations	Medium
Excessive data processing; the data processed needs to be proportionate to the deployment of LFR. Particularly for those passing through the Zone of Recognition, if the data is not really needed (i.e. not all cameras are needed) and could be removed from the use of LFR without undermining its delivery, there is a danger of unjustified collateral intrusion.	High	Likelihood of risk reduced due to mitigations	Medium
Irrelevant data processing; if LFR uses more data than it needs to achieve its aim, this would intrude into people's private lives where there wasn't a need to do so and it risks undermining trust and confidence in BTP.	High	Likelihood of risk reduced due to mitigations	Medium

• if the image quality is not sufficient to generate True Alerts, such data risks increased False Alerts and unwarranted Engagements with data subjects; • if Sought Persons are added to the Watchlist where the matter has been resolved by other means, this risks unwarranted engagements as a result of irrelevant data being processed.			
Inaccuracies in the data itself; the data should be accurate, and where necessary, kept up to date with systems in place to erase or correct errors as needed. Inaccuracies in the data risk those added to an LFR Watchlist being subject to unwarranted Alerts/Engagements and could result in unlawful detention.	High	Likelihood of risk reduced due to mitigations	Medium
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 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.	High	Likelihood of risk reduced due to mitigations	Medium
Inaccuracies in the algorithm – if the algorithm is inaccurate then this may adversely impact on the data subject in a number of ways including; Unnecessary data processing where the algorithm could be assessed upfront to be an unviable proposition to policing; Potential impact on individuals passing through the zone of	High	Likelihood of risk reduced due to mitigations	Medium

recognition especially in the context of false alerts; A failure to achieve the objectives for LFR such that data is needlessly being processed if the LFR system is not able to reliably generate true alerts.			
As a result of limited availability of images for testing the software there is 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.	High	Likelihood of risk reduced due to mitigations	Medium
Data Retention; there is a risk that if the retention periods in the Policy are not applied and the data is not subject to meaningful review, it is retained where there is no need to do so.	High	Likelihood of risk reduced due to mitigations	Medium
Data Security; People's privacy and wider interests can be put at risk if their personal data is not protected by adequate technical and security measures from both internal and external risks. For those on the Watchlist, and those passing through the Zone of Recognition, if biometric data is not adequately protected, its unique nature to enable identification means if there is a security breach, it is liable to exploitation by malactors. For those on a Watchlist, a data breach may confirm that a subject has been on an LFR Watchlist or their data has been retained because they are subject to an Alert. This could be used to impact on the	High	Likelihood of risk reduced due to mitigations	Medium

individual should it fall into the hands of malactors			
Data Loss; If data is not accessible or otherwise corrupted (through unlawful action or accident) it may undermine the ability to deploy LFR. It may also prevent the BTP acting on, and reporting on the results of an LFR deployment.	High	Likelihood of risk reduced due to mitigations	Medium
Data Subject Rights requests; 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	Medium	Likelihood of risk reduced due to mitigations	Low
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.	Medium	Residual risk remains	Medium
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.	High	Likelihood of risk reduced due to mitigations	Medium
There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court	High	Likelihood of risk reduced due to mitigations	Medium

cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action.			
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	High	Likelihood of risk reduced due to mitigations	Medium
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	High	Likelihood of risk reduced due to mitigations	Medium
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.	Medium	Likelihood of risk reduced due to mitigations	Low
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	Medium	Likelihood of risk reduced due to mitigations	Low

potential breaches of the DPA'18 which may result in enforcement action, legal action and financial penalties			
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	High	Likelihood of risk reduced due to mitigations	Medium

Section 6: Review

A DPIA is not a process that ends at sign off or at go live of a project. Please outline the review process that you will undertake to ensure that the mitigations have been successful and no new risks have been identified during implementation.

6.1 Responsibility for implementing mitigations

Who will be responsible for ensuring that all listed mitigations have been implemented in practice? This could be more than one person – list all below as applicable. What is the expected date of completion for any actions required?

Action/Mitigation	**Assigned to (SIRO/IAO/SO):**
A. Full pre-deployment assessment (including approving the case use, watchlist composition etc)	LFR Authorising Officer (LFRAO) & LFR Bronze / Silver / Gold
B. Creation of Watchlist	FIB (Intel)
C. Manual Adjudication and deletion of images from watchlist during deployment	LFR operators
D. Full post-deployment review	LFR Gold / Silver / Bronze

6.2 Responsibility for reviewing impact of mitigations

Who will be responsible for ensuring that the mitigations have successfully reduced risk as expected? When is this review scheduled for?

Action/Mitigation	**Review Date:**
A. Full pre-deployment assessment (including approving the case use, watchlist composition etc)	LFR Bronze / Silver / Gold
B. Creation of Watchlist	LFRAO
C. Manual adjudication and deletion of images from watchlist during deployment	LFRAO
D. Full post-deployment review	LFR Gold / Silver / Bronze

6.3 Roles and Responsibilities

Team	**Role**

FIB	* Produces intelligence case for LFR use covering each relevant period. * Produces watchlists.
A&I DATA SERVICES MANAGER	* Produce Neoface compatible watchlists.
LFRAO	* Authorises LFR use.
LFR OPERATORS	* Reviews watchlists for protected characteristics * Operates LFR system
LFR GOLD	* Strategic responsibility for LFR operations * Authorises the final watchlist
LFR BRONZE	* Operational responsibility for LFR operations
LFR SILVER	* Tactical responsibility for LFR operations
HEAD OF INTEL	* Approves the final watchlist sent to the LFR team 24 hours before deployment
Once you have completed all sections above as applicable, the completed assessment should be submitted to the Force Data Protection Officer for advice and sign off. Please send the completed assessment to informationsharing@btp.police.uk No processing of information should begin until an outcome has been received.	

Section 7: Outcome

DPO Advice/Outcome

This assessment has set out all of the applicable risks and mitigations and risk levels have been mitigated to acceptable levels. The next step is intended to be a pilot of deployment of LFR in operational scenarios. The pilot will demonstrate operational effectiveness and allow the Data Protection Impact Assessment to be evaluated and updated as necessary. There should therefore be ongoing and iterative review of this assessment during the pilot period.

Advice Provided By: Deputy Data Protection Officer	Date: 10/02/2026