Data Protection Impact Assessment Report (DPIA2)

Project Information	
Project Name (and or number)	Hampshire & Isle Of Wight Constabulary (HIOWC) Live Facial Recognition (LFR)
Forces involved in Project	Hampshire & Isle of Wight Constabulary
Information Asset Owner	Detective Chief Superintendent Tim Rowlandson - Head of Intelligence & Serious Organised Crime - (LFR) Tom Kempster Head of Technology Innovation (RMS)
Senior Responsible Officer	ACC Paul Bartolomeo – Crime & Criminal Justice and Intelligence
Project Manager	Abbie Newnham – Corporate Insights
Information Governance - JIMU Contact	Sharon Warwick – Senior Information Governance Manager

Document Ownership	
Author(s)	Nicola Cain – Principal Consultant, Handley Gill Limited
Document Owner	Sharon Warwick – Senior Information Governance Manager

Document Review Information			
Version History	**Version Date**	**Requestor of Change**	**Summary of Change(s)**
0.1	05/08/2024	N/A	First Draft
0.2	22/08/2024	Nicola Cain	Amendments needed on first draft
1.0	01/09/2024		Final changes for publication – proof of concept trial
2.0	05/12/2025	Sharon Warwick	Review ahead of next LFR use December 2025

Data Protection Impact Assessment Report

1. Outline of the project, objectives, benefits and purpose

HIOWC proposes to commence and embed the operational capability of overt, intelligence-led Live Facial Recognition ('LFR') deployments commencing December 2025

The LFR deployments will be delivered using specialist equipment operated by the Hampshire & Isle of Wight Constabulary and Thames Valley Police collaborated Joint Operations Unit, LFR Team. During the preparation and delivery of a specific LFR deployment the LFR Team will be acting under the direction and control of the Chief Constable (as data controller) that is requesting the deployment in their force, according to the arrangements set out in their own LFR Policy and Standard Operating Procedure and other associated LFR impact assessments and documents.

Live Facial Recognition is the live capture by video camera of facial images which are subjected to biometric analysis in real time and are cross-matched against a database or watchlist of images - usually drawn from existing police assets - of individuals, from which a biometric template has been extracted, to identify potential matches (subject to the configured thresholds for accuracy).

The deployments will be delivered through the specialist equipment purchased for this purpose across HIOWC and Thames Valley Police and the deployment of a bi-lateral LFR team. In the event of a match being identified and affirmed by the LFR operators, engagement officers will seek to intercept the relevant match to confirm their identity and take any necessary action.

It is anticipated that the deployments will serve a number of functions, primarily by supporting HIOWC to:

a) Locate persons currently wanted for offences who have an outstanding warrant for their arrest issued by a court or are sought for recall to prison.
b) Locate individuals who are missing and considered at increased risk of harm where HIOWC has assessed it as:
    - Medium risk: where the risk of harm to the subject or public is assessed as likely but not serious.
    - High risk: where the risk of serious harm to the subject or the public is assessed as very likely.
c) Locate individuals shown as outstanding suspects for a range of criminal offences, including high risk crimes and those relating to local district priorities which justifies the inclusion.
d) Prevent or reduce crime in and in the vicinity of the deployment locations

The conduct of targeted patrols in priority hotspot areas by uniformed officers has previously been carried out by HIOWC in an effort to achieve these aims under the auspices of Operation SENTINAL. This operation, which focuses on the reduction of serious violence, was funded by the Home Office, but there continues to be high numbers of wanted individuals at large and significant crime commission rates in priority hotspot areas across the county. It is proposed that the LFR tactic will support the

prevention and detection of crime in these and other hotspot locations. A separate campaign, Operation Relentless, is periodically undertaken in an effort to identify and reduce the number of outstanding suspects of crime and persons wanted on warrant across the constabulary. These periods of focused operational activity regularly lead to reductions in overall outstanding suspect numbers and LFR will be a valuable tactic to support Operation Relentless and other, more regular operations.

As recognised in the Retail Crime Action Plan launched in October 2023, violent crime coupled with acquisitive crime has been increasing, particularly in a retail context. The Plan specifies that *"Analytics of Police National Computer (PNC) / Police National Database (PND) data, including crime scene facial recognition data, should be used to identify prolific offenders and proactively pursue them from a criminal justice perspective"*. The subsequent 'Fighting retail crime: more action' report published by the Home Office in April 2024 advocated greater use of facial recognition technologies, including live facial recognition, to tackle retail crime.

The use of facial recognition as a technological tool to exploit existing police and law enforcement assets to respond to the rising threat of serious acquisitive crime was also identified in the 2022 HMICFRS' report 'The police response to burglary, robbery and other acquisitive crime – Finding time for crime'.

The individuals who may be affected by the deployment will be:

- Individuals whose image is included in the LFR deployment watchlist and whose personal data is processed;
- Individuals who avoid entering the zone of recognition and whose personal data is not processed;
- Individuals who enter the zone of recognition but whose image is not captured by the LFR system and whose personal data is not processed;
- Individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system but are not the subject of an alert and whose personal data, including biometric data (comprising special category data/sensitive processing) is processed;
- Individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert representing a potential match which is discounted as false by the operator and whose personal data is processed, including biometric data (comprising special category data/sensitive processing);
- Individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by the operator and referred to the intervention officer on the ground but no contact is made and whose personal data is processed, including biometric data (comprising special category data/sensitive processing);
- Individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by the operator and referred to the intervention officer on the ground with contact being made but the officer confirms the individual is not the wanted individual, and personal data is processed, including biometric data (comprising special category data/sensitive processing);
- Individuals who enter the zone of recognition and whose image is captured and ingested into the LFR system who are the subject of an alert which is affirmed by

the operator and referred to the intervention officer on the ground with contact being made and the officer confirms the individual is the wanted individual and arrests or otherwise disposes of the matter, and personal data is processed, including biometric data (comprising special category data/sensitive processing).

The proposed processing activities will be conducted pursuant to Part 3 Data Protection Act 2018 and/or, particularly in connection with missing persons considered at increased risk of harm, the UK GDPR.

While all of these categories of individual are considered in the Human Rights Impact Assessment and Equality Impact Assessment, which have been conducted contemporaneously with this Data Protection Impact Assessment (DPIA), only those categories of individual whose personal data may be processed in the course of the deployment are addressed in this DPIA.

LFR is not a new policing tactic and has been deployed in other forces as well as piloted in HIOWC. Regard has been had to the LFR deployments carried out in other police forces, to inform the location and circumstances of the deployment as well as the technical configurations of the LFR equipment that will ensure that the deployments can be effective while protecting the data protection and human rights of affected individuals.

Considering LFR deployments by other forces:

- the Metropolitan Police Service since 2023 (between the period 06 April 2023 – 23 July 2024, as per the current published deployment records), has arrested 337 individuals across 122 deployments following engagements as a result of LFR, in addition to instances where other disposals or no further action was taken. It is recognised that the MPS has deployed LFR during this period at thresholds lower than that at which HIOWC will deploy LFR (at configurations of 0.6 and 0.62, whereas Hampshire will, in general, not use a threshold of less than 0.64) and that the highest false alert rate (calculated as a proportion of the total number of faces seen by the system) recorded during that period was 0.18% utilising watchlist of c.9,500 – 15,000 individuals; and,
- South Wales Police throughout 2023 to 15 November 2025 (time of writing) has deployed LFR at a configuration threshold of 0.64 and has had an incorrect alert rate of 0 throughout that period.

During the pilot in HIOWC it was identified that the use of LFR was a likely significant contributory factor to low crime commission in the areas and at the times of deployments.

Having regard to these outcomes, the scientific research detailed further below, and the intelligence led approach to the proposed deployments, it is anticipated that at the threshold setting of 0.64 (a deliberate decision set out in the LFR policy to accept and implement a low tolerance for false matches at a level which also minimises or extinguishes the risk of bias or discrimination) and curated watchlists likely to be no greater than 3,000 with an emphasis being placed on streamlining the watchlist in so far as is consistent with achieving the purpose), it is anticipated that not only will the deployments result in the arrest or other disposal of wanted individuals but that they will

also serve to deter, prevent or reduce crime. The effectiveness of the pilot deployments will be monitored against these measures.

The deployments will serve to deliver the administration of justice, make the public safer and improve public confidence in policing. The deployments are expected to support HIOWC in achieving its priorities of relentlessly pursuing criminals, delivering exceptional local policing and putting victims first.

It is intended that all individuals who approach the perimeter of the LFR deployment will be made aware of the deployment through signage, and this will be in the context of a wider awareness campaign.

It is anticipated that the majority of individuals who approach the perimeter will continue on to enter and may pass through the zone of recognition, potentially resulting in their image being captured and a biometric template extracted and compared with those on the LFR watchlist.

For those individuals whose personal data is processed but who are not matched, their personal data will be processed with their knowledge in the form of the CCTV images of them as a result of the measures to be taken by the force, and a biometric template which will be extracted from the image and compared with the biometric templates of the watchlist images. The biometric template will be deleted automatically and almost instantaneously. CCTV images will be retained for 31 days, unless retention for a longer period is warranted, for example in the event of a complaint.

As a consequence of the public awareness campaign to be carried out as part of each deployment, individuals will be alerted to their rights and methods of recourse in respect of the processing of their personal data. In practice, however, the processing of personal data of these individuals should have a limited impact at the proposed configuration thresholds, comprising the short-term processing of their personal data with the most sensitive biometric data being promptly deleted.

In relation to individuals whose personal data is processed and in respect of whom a potential match is flagged, their personal data will be processed with their knowledge in the form of the CCTV images of them as a result of the measures to be taken by the force, and a biometric template will be extracted from the image and compared with the biometric templates of the watchlist images. If the operator reviews the potential match but does not affirm the match, no engagement with the individual will be undertaken by officers. While the biometric template of such individuals will not be immediately deleted, it will be deleted within 24 hours of the conclusion of the deployment. The CCTV images will be retained for 31 days and may be retained for a longer period where justified in the event of a complaint or prosecution, for example.

In all cases, deployment logs that do not contain personal data will be retained for 6 years.

In relation to individuals whose personal data is processed and in respect of whom a potential match is flagged, their personal data will be processed with their knowledge in the form of the CCTV images of them as a result of the measures to be taken by the force, a biometric template will be extracted from the image and compared with the

biometric templates of the watchlist images. If the operator reviews the potential match and affirms the match, a decision will be taken by HIOWC/LFR officers as to whether to seek to engage the individual and officers will then seek to carry out an engagement, with a view to verifying the identity of the individual and taking any appropriate action, such as arrest or other disposal where individuals are wanted on warrant or suspicion of the commission of a serious or priority offence, or to safeguard the individual in the case of missing persons considered at increased risk of harm.

The process of matching a biometric template, which is then double verified, first by the LFR operator and subsequently by the engagement officer prior to an engagement being effected, implements additional safeguards for individuals against being wrongly identified compared to seeking to identify individuals by officers on sight alone. The adoption of LFR should ensure that there are fewer inappropriate interventions while increasing the rate of apprehension of wanted individuals.

This DPIA forms part of a suite of documents which detail the approach and assessment of various risks and mitigations in relation to the deployment of LFR, the HIOWC LFR Documentation including this DPIA should be read in conjunction with those documents, in particular the HIOWC LFR Legal Mandate, HIOWC LFR Policy, HIOWC LFR SOP, HIOW LFR Retention Schedule, HIOWC LFR Appropriate Policy Document, HIOWC LFR Human Rights Impact Assessment, HIOWC LFR Equality Impact Assessment and, Surveillance Camera Assessment as well as the specific LFR Deployment Application and Authorisation.

This documentation has been prepared having regard to existing law, jurisprudence and guidance (binding or otherwise) including: the UK GDPR; the Data Protection Act 2018; the Human Rights Act 1998; the Equality Act 2010; the Protection of Freedom Act 2012; the Amended Surveillance Camera Code of Practice; the Covenant for Using Artificial Intelligence (AI) in Policing; the Biometrics and Forensics Ethics Group Facial Recognition Working Group Interim Report; Information Commissioner's Opinion on 'The use of live facial recognition technology by law enforcement in public places'; Ada Lovelace Institute 'Beyond face value: public attitudes to facial recognition technology'; R (On the application of Edward BRIDGES) v (1) The Chief Constable of South Wales Police and (2) The Secretary of State for the Home Department and others [2020] EWCA Civ 1058; Surveillance Camera Commissioner's 'Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales'; Information Commissioner's Opinion on 'The use of live facial recognition technology in public places'; Council of Europe Guidelines on facial recognition; College of Policing Authorised Professional Practice on Live Facial Recognition; Global Privacy Assembly Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology; European Data Protection Board 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement'; Glukhin v Russia (Application no. 11519/20); A Guide to Using Artificial Intelligence in the Public Sector; and, the UNESCO Recommendation on the Ethics of Artificial Intelligence.

2. Describe the intended use of personal data:

a) Describe the nature of the processing:

The categories of personal data processed in the course of an LFR deployment will comprise:

- Images of individuals for inclusion in the watchlist;
- Extracted biometric templates of individuals included in the watchlist
- CCTV images of individuals passing through the zone of recognition;
- Extracted biometric templates of individuals passing through the LFR zone of recognition;
- Flagged matches;
- Logs and records pertaining to consideration of matches and any engagement undertaken with individuals.

Categories of special category personal data that may be processed/sensitive processing that may be undertaken in the course of an LFR deployment comprise:

- Racial or ethnic origin;
- Religious or philosophical beliefs;
- the processing of biometric data for the purpose of uniquely identifying a natural person;
- data concerning health.

Processing will also include criminal conviction and offence data.

It is acknowledged that the processing of personal data in the context of LFR deployments will involve the use of novel technologies, in particular the use of artificial intelligence in the form of the extraction and comparison of biometric templates of still and moving images. The specific technology to be used in the HIOWC LFR deployments has, however, been subject to scientific testing both as to its efficacy (by the US National Institute of Standards and Technology (NIST)) and to identify any potential bias or discrimination (by the UK's National Physical Laboratory), and the results of these tests are published, have been reviewed and taken into account in the context of this DPIA, the wider HIOWC LFR Documentation and the HIOWC LFR deployments, and are referenced in further detail as appropriate below.

LFR watchlist images will usually be obtained from existing police and law enforcement records, in particular custody images, which are taken in circumstances where the affected individuals are aware of the collection of their personal data and its retention and use is already subject to various laws and regulations. While this processing is not based on consent, and individuals may not have been aware of the potential for their image to be used in the context of an HIOWC LFR deployment, as the technology has emerged relatively recently, the use of their custody images for further law enforcement purposes including the investigation and prosecution of crimes would have been within their reasonable expectations and, where offences have been committed, is the inevitable consequence of those actions.

However, in circumstances where a recent suitable quality custody image is unavailable, consideration may be given to using an alternate image. This could be in circumstances where a missing person considered at increased risk of harm is proposed to be included on a watchlist and an image is provided by their family or

obtained from social media or CCTV. It is acknowledged that such images may impact on the performance of the LFR system. Ensuring the quality of images included on the watchlist does not reduce the performance of the LFR system is the responsibility of the LFR Silver Commander to ensure the following safeguards are implemented per deployment:

a) The most up to date custody images or non-police sourced images of a person who meets the criteria for inclusion on the watchlist will be extracted for LFR use.
b) By using image 'ingestion settings' (such as: distance between eyes, facial quality and facial reliability, face tilt) that have proven to be reliable the LFR System has a technical safety net exist to prevent images of poor quality from being uploaded onto the LFR system.
c) Reviewing the proposed watchlist images prior to uploading, with particular attention paid to non-police sourced images (e.g.: for high risk missing persons), in combination with the briefing of LFR Operators and Engagement Officers so that they are mindful of the limitations and implications of its use.

Biometric templates are then extracted from the images once the data is uploaded to the LFR System. Watchlists will not be uploaded more than 24 hours prior to a deployment to ensure that the watchlist is as current as is practically reasonable.

CCTV images are then obtained of the zone of recognition through which individuals will pass. The LFR System detects a face/s within the CCTV images (which may be affected by factors including crowd density, lighting conditions and the individual's own behaviours and any accoutrements) and that face is 'enrolled' into the LFR System. The LFR System automatically extracts biometric templates from the CCTV images of individuals passing through the zone, which may occur multiple times as individuals pass through, and will then automatically compare and seek to match those biometric templates against the watchlist.

CCTV footage shall be retained on HIOWC systems in accordance with MOPI for a minimum of 31 days following a deployment and longer if required.

Biometric templates of individuals who are not flagged as a potential match are automatically and almost instantaneously deleted by the LFR system. Biometric templates of individuals who are flagged as a potential match are deleted within 24 hours of the conclusion of the deployment.

Where individuals are flagged as a potential match for individuals on the watchlist, this results in the three thumbnail images being returned and saved comprised of the input image, the CCTV frame, and the image of the extracted face, together with related metadata. This information will be assessed by the LFR Operators to make a recommendation to LFR Engagement Officers as to whether to seek to engage the individual to conduct further checks. The LFR system does not determine whether an individual should be stopped, arrested or subjected to other action.

All watchlist images uploaded to the LFR system are deleted within 24 hours of the conclusion of the deployment (albeit the originating images will continue to be retained in accordance with MOPI).

The National Police Chief Councils (NPCC) Authorised Professional Practice (APP) on Information Management governs the retention of the source custody images stored on the HIOWC's crime recording systems, from which the watchlist images are extracted.

Where non-police sourced images are included on the watchlist (for example: to locate missing persons considered at increased risk of harm) they will have previously been obtained from family / friends / associates. The retention of non-police sourced images, beyond being used for LFR, will be managed according to the NPCC APP on Information Management.

Logs and other documentation, that does not contain personal data, relating to the LFR Deployment are retained for 6 years.

Within the LFR system, this is a stand-alone and non-networked system, which is subject to security measures, including: the LFR application has two layers of password protection to access the application; the LFR application is staffed when in use and therefore physical protections are in place; LFR system engineers are deployed with the system when in operation; deployment data stored on the system is securely wiped following each deployment; individual users of the LFR application and subject to role based access controls with limited user permissions; the dashboard and RESTful API are secured with SSL and TLS by default, and all connections are directed through HTTPS; the LFR application can be connected to mobile devices using a private access point with three levels of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App; and logging data is retained of user activity which enables auditing to be conducted.

Watchlist images are transferred to the system using an encrypted USB memory stick, which is deleted within 24 hours following the conclusion of each LFR deployment.

Other data held on HIOWC systems is held in accordance with MOPI and HIOWC information security policies and procedures.

The Chief Constable of HIOWC is the data controller in respect of personal data processed in the context of its LFR Deployments at all times.

b) Describe the scope of the processing:

The processing will concern:

- Custody images of individuals included on the deployment watchlist, which may include images of children/vulnerable people;
- Other images of individuals included in the deployment watchlist, which could include non-police sourced images, and which may include images of children/vulnerable people;
- Biometric templates of individuals included in the deployment watchlist;
- CCTV images of individuals entering the LFR Deployment zone of recognition and captured by the LFR cameras;

- Biometric templates of individuals entering the LFR Deployment zone of recognition and captured by the LFR cameras;
- Information relating to any potential match flagged by the LFR system;

The personal data processed will relate to the following categories of individual:

- Individuals convicted of criminal offences;
- Individuals suspected of the commission of criminal offences;
- Victims of criminal offences;
- Missing persons considered at increased risk of harm;
- Members of the public in the vicinity of the LFR deployment;
- Children and/or vulnerable people falling within the above categories.

Personal data of police officers and staff may also be processed.

In relation to individuals included on a watchlist, it is anticipated that this could include hundreds or potentially thousands of individuals per deployment. It is assumed for the purpose of this DPIA that no list will include more than approximately 3,000 individuals. Individuals whose personal data is processed may be more likely to be locally based but processing is not restricted to individuals who reside in HIOW. LFR deployments will take place in targeted locations deemed appropriate and proportionate for this tactic.

As an example to the anticipated scale of processing, having regard to the anticipated size of the watchlist, publicly available data on city centre footfall (which suggests that average daily footfall in Portsmouth City Centre is approximately 20-25,000), the limited zone of recognition of deployments, and the average number of faces seen by other forces when conducting deployments in the context of the publicly available data on population size (in excess of 200,000), it is anticipated that a deployment would impact less than 10% of the population and that for the vast majority of such individuals the processing will last no longer than the time it takes them to traverse the LFR zone of recognition before their personal data is deleted and the impact on them is considered to be negligible, and that the most intrusive processing would potentially impact only 1% of the population approximately.

As detailed further below, steps are taken to minimise the duration of processing of personal data. In respect of the most sensitive biometric data, in respect of individuals who are not flagged as a potential match for a watchlist image, this data is deleted automatically and almost instantaneously. In relation to biometric templates of individuals who are flagged as potential matches, the biometric template is deleted no later than 24 hours following the conclusion of the deployment, whereas LFR Operator logs in relation to the flagged match are retained for 6 years to ensure there is an appropriate record. CCTV images are deleted 31 days after deployment unless there is a reason for retention.

c) Describe the bigger picture in which the processing is taking place:

The use of LFR has been the subject of considerable debate, in public and in Parliament, has been considered by the courts and is frequently attacked by civil society organisations who have raised concerns not only regarding individual deployments but of the risks of the proliferation of LFR and the implications for individual privacy.

Successive governments have concluded that it is not necessary to introduce bespoke legislation governing LFR, and this is therefore subject to a range of laws and regulations which are detailed in this DPIA and the wider HIOWC LFR documentation. The courts have acknowledged that the deployment of LFR can be lawful in circumstances where the parameters in which it operates are suitably prescribed and published. The courts have recognised the importance to society of tackling crime and it is the duty of the police to undertake this role. Individuals who are included in watchlists are individuals who have either been identified as being wanted by the courts, for recall to prison or on suspicion of the commission of a range of offences including high risk crimes and those relating to district priorities, or for safeguarding reasons for missing persons considered at risk of harm. In neither case will these individuals have consented to the processing of their personal data and, indeed, they may vociferously object to such processing given the choice. Nevertheless, there is a clear and strong public interest in identifying such individuals and enabling them to be subject to appropriate action. In light of the existing measures that HIOWC takes, it is considered that the further/use of images for law enforcement purposes is likely to be within individuals' expectations (even if the use of LFR was not at the time of the original collection of images) and that the specific supplementary measures connected with LFR deployments to notify individuals about LFR ensure that the processing is suitably transparent. In relation to missing persons considered at increased risk of harm, the need to safeguard their interests outweighs any reasonable expectations they might have in relation to the privacy of non-police images, albeit that non-police sourced images require particularly careful consideration.

3. Data Subject Views:

Careful consideration has been given to the views of the general public in relation to the deployment of LFR, which is acknowledged to be a relatively new technology which may not be readily understood. It is noted that in September 2019, the Ada Lovelace Institute published the results of its national survey of public attitudes to facial recognition technology, 'Beyond face value', which revealed that *"the British public are prepared to accept use of facial recognition technology in some instances, when there is a clear public benefit and where appropriate safeguards are put in place, but they also want the government to impose restrictions on its use"*. Regard has also been had to consultations carried out in other police force areas, including the work of the London Policing Ethics Panel survey the results of which were referenced in its May 2019 final report on Live Facial Recognition. The Information Commissioner's own survey conducted in 2019 revealed that 82% of those surveyed indicated that it was acceptable for the police to use LFR, 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime and, 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.

It is acknowledged that both of these surveys are now somewhat outdated and that the reliability and accuracy of the relevant technology has improved in the ensuing five-year period and that LFR has been adopted more widely by both law enforcement and other sectors and is therefore more commonplace, as is AI more generally, and is therefore likely to be better understood by at least sections of the public.

More recently, research conducted on behalf of the Department for Science, Innovation and Technology in its 'Public attitudes to data and AI: Tracker survey (Wave 3)' published in February 2024 revealed that 44% of the public believed that AI would have a positive impact on the prevention and detection of crime, while 29% were neutral.

We are mindful of concerns raised by civil society groups in particular to LFR, and have carefully considered the judgment of the Court of Appeal in R (On the application of Edward BRIDGES) v (1) The Chief Constable of South Wales Police and (2) The Secretary of State for the Home Department and others [2020] EWCA Civ 1058, and subsequent legal challenges by these groups and individuals they support, as well as the judgment of the European Court of Human Rights in Glukhin v Russia (Application no. 11519/20), and the concerns and guidance raised have been addressed in the design of and implementation of safeguards applicable to the deployments.

Specifically in the police force area of Hampshire and the Isle of Wight, several preliminary consultations have been carried out and it is intended that an ongoing process of consultation/feedback throughout the period of and following the deployments with these and other groups and individuals will be carried out:

- Force Strategic Independent Advisory Group: the HIOWC Force Strategic Independent Advisory Group is an independent specialist advisory group made up of volunteers and a chair. The chair of the group was updated on the 19th November 2025 regarding HIOWC's intention to add LFR to its existing range of policing tactics so that it can be deployed, when needed and is appropriate to do so, as a mainstream this tactic from December 2025 onwards.
- HIOWC Ethics Committee: In September 2025 the HIOWC Ethics Committee, which is comprised of members of the public, staff representative groups and leaders within the police force, was briefed on the proposed deployments;

Police and Crime Commissioner (PCC): on 25th November 2025, the elected PCC for Hampshire and the Isle of Wight, Donna Jones, was briefed on this updated proposal at the Joint Chief Constable and PCC Collaboration Governance Board.

No objections have been received to the proposed deployments.

The Information Commissioner's Office was notified of HIOWC's intention to use LFR, in advance of initial deployments.

Through the on-the-ground engagement by officers with members of the public during the course of deployments, and as a consequence of the associated publicity, it is anticipated that unsolicited feedback will be provided which will further inform our view of public attitudes. This could be supplemented with targeted consultations, including the individuals and groups identified above as well as other groups, such as HIOWC's Strategic Youth Independent Advisory group.

It is acknowledged that individuals likely to be included as part of watchlists have not been the subject of explicit pro-active consultation; this is because it would be either impossible or inappropriate to carry out such consultation.

4. Data protection compliance – assessment of necessity and proportionality of personal data processing.

Information is being processed under UK GDPR & Law Enforcement rules

Principle 1: Use of personal data is fair, lawful, and transparent:

- Lawful basis for the processing of personal data under applicable data protection legislation as stated as follows:
- Personal data:
  - where processing takes place pursuant to Part 3 Data Protection Act 2018, i.e. for the law enforcement purposes, the processing of personal data takes place in accordance with section 35(2)(b) Data Protection Act 2018, i.e. the processing is necessary for task carried out for the law enforcement purposes by HIOWC, which is a competent authority for the purposes of the Act;
  - where processing takes place pursuant to the UK GDPR, the processing meets one or more of the following requirements: processing is necessary for compliance with a legal obligation to which the controller is subject [Article 6(1)(c) UK GDPR]; processing is necessary to protect the vital interests of the data subject or another natural person [Article 6(1)(d) UK GDPR]; and/or processing is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6(1)(e) UK GDPR].
- Special Category data/Sensitive processing:
  - where sensitive processing takes place pursuant to Part 3 Data Protection Act 2018, the processing takes place in accordance with section 35(5) Data Protection Act 2018, i.e. the processing is strictly necessary for the law enforcement purpose, HIOWC has an appropriate policy document in place and the processing meets a Schedule 8 condition, i.e. one or more of the following applies: the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest [Schedule 8 paragraph 1]; processing is necessary for the administration of justice [Schedule 8 paragraph 2]; processing is necessary to protect the vital interests of the data subject or of another individual [Schedule 8 paragraph 3]; processing is necessary for the safeguarding of children or individuals at risk [Schedule 8 paragraph 4]; processing relates to personal data manifestly made public by the data subject [Schedule 8 paragraph 5]; and/or processing is necessary for the purposes of or in connection with legal proceedings [Schedule 8 paragraph 6(a)];
  - where processing of special category data takes place pursuant to the UK GDPR, this shall meet one or more of the following requirements:

processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Article 9(2)(c) UK GDPR]; processing relates to personal data which are manifestly made public by the data subject [Article 9(2)(e) UK GDPR]; and/or 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) UK GDPR] and meets one or more of the following conditions of Part 2 Schedule 1 Data Protection Act 2018 and an appropriate policy document is in place: the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 6]; the processing is necessary for the administration of justice [Part 2 Schedule 1 paragraph 7]; processing relates to a specified category of personal data and is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained [Part 2 Schedule 1 paragraph 8]; processing is necessary for the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as to not prejudice those purposes and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 10]; processing is necessary for the purpose of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act [Part 2 Schedule 1 paragraph 12]; and/or processing is necessary for the purposes of safeguarding children and individuals at risk [Part 2 Schedule 1 paragraph 18].

- Criminal data: where criminal conviction and offence data is processed pursuant to the UK GDPR, this shall be carried out in accordance with article 10 UK GDPR and section 10(5) Data Protection Act 2018 and shall meet one or more conditions set out in Schedule 1 Parts 1-3: an appropriate policy document shall be in place and one or more of the following conditions are met: the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 6]; the processing is necessary for the administration of justice [Part 2 Schedule 1 paragraph 7]; processing relates to a specified category of personal data and is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained [Part 2 Schedule 1 paragraph 8]; processing is necessary for the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as to not prejudice those purposes and is necessary for reasons of substantial public interest [Part 2 Schedule 1 paragraph 10]; processing is necessary for the purpose of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act [Part 2 Schedule 1 paragraph 12]; and/or

processing is necessary for the purposes of safeguarding children and individuals at risk [Part 2 Schedule 1 paragraph 18]

- Wider lawfulness
  While the wider lawfulness of the processing of personal data in the context of the proposed overt deployment of LFR is addressed in detail in the HIOWC LFR Legal Mandate, which should be read in conjunction with this DPIA, the position is summarised below.

It is acknowledged that there is no specific legislation in this jurisdiction which regulates the development or deployment of artificial intelligence generally, or live facial recognition technologies specifically, but that these are governed or informed by existing laws and guidance, including the Data Protection Act 2018, UK GDPR, Human Rights Act 1998, Equality Act 2010, Protection of Freedoms Act 2012, the Amended Surveillance Camera Code of Practice, the Surveillance Camera Commissioner's 'Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a watchlist, in Public Places in England & Wales', Information Commissioner's Opinion on 'The use of live facial recognition technology in public places', the College of Policing Authorised Professional Practice on Live Facial Recognition, and jurisprudence.

In addition to complying with the specific requirements of data protection legislation, steps have been taken to ensure that the proposed processing meets wider legal obligations, including under the Human Rights Act 1998 and Equality Act 2010.

The Court of Appeal in Bridges recognised that *"the legal framework which regulates the deployment of AFR Locate does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary"* [69], however that framework was considered to be *"insufficient"* [90] on the basis that *"too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed"* [91]. The Court accepted, however, that *"in principle a police force's local policies can constitute relevant "law" in the present context, provided they are published"* [121].

Subsequent to that judgment, the College of Policing has published its APP on Live Facial Recognition and HIOWC has supplemented this with the HIOWC LFR Documentation, including the LFR Policy, LFR SOP and LFR Application and Authorisation, which explicitly address not only the categories of individual liable to be placed on a watchlist (with, incidentally, HIOWC adopting a narrower scope than is permitted under the APP), and factors relevant to the identification of appropriate LFR Deployment locations, but also define the parameters within which the LFR System is permitted to be operated. It is notable that it is a feature of the LFR System that the biometric templates of individuals which are sought to be matched against the watchlist but which do not result in a potential match are automatically and almost instantaneously deleted and, were it not a feature, it would be a requirement of the HIOWC LFR Documentation that this be the case.

The European Convention on Human Rights and the Human Rights Act 1998, which incorporates Article 8 of the Convention into UK law, protects the right to respect for private and family life. While the European Court of Human Rights has held that the use of LFR constituted a violation of Article 8 ECHR, notwithstanding its finding that *"beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification",* this was in circumstances where the offence under investigation was of a minor, administrative nature, utilised social media images (rather than images already lawfully held by the police/law enforcement) to identify him, and national laws were considered to permit unfettered use of LFR.

The Amended Surveillance Camera Code of Practice requires that *"a system is demonstrably being operated in a manner which has regard to the SC Code and such regard is supported by an appropriate audit trail"*. HIOWC has carried out a Surveillance Camera Code Assessment, which should be read in conjunction with this DPIA.

s.149 Equality Act 2010 imposes an obligation on public authorities, including chief officers, in the exercise of their functions to have due regard to the need to eliminate discrimination, harassment, victimisation and other forms of prohibited, advance equality of opportunity between those who share a protected characteristic and those who don't and, to foster good relations between such groups.

Sections 13 and 19 Equality Act 2010 prohibit direct (that is to say the less favourable treatment of a person compared to another based on a protected characteristic (i.e. age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and/or sexual orientation)) and indirect (the application of a provision, policy or practice to an individual discriminates against them based on a relevant protected characteristic (these are all of the protected characteristics identified above with the exception of pregnancy and maternity)) discrimination respectively.

In support of meeting this duty (the public sector equality duty (PSED)), and ensuring that LFR Deployments are not discriminatory, HIOWC has carried out an LFR Equality Impact Assessment (EIA) which shall be reviewed at least annually and kept under periodic monitoring throughout the period during which LFR Deployments are undertaken to ensure that any learning or trends can be identified and addressed at an early stage. That EIA should be read in conjunction with this DPIA and the Human Rights Impact Assessment in particular.

Specifically in connection with the processing of personal data, however, consideration has been given to any potentially discriminatory impact of the operation of the LFR system. In carrying out this assessment, the results of the National Physical Laboratory report 'Facial Recognition Technology in Law Enforcement Equitability Study' (2023), assessing the NEC Neoface V4 1 using HD5 Face Detector which is the HIOWC LFR system, have been analysed. The study assessed the efficacy and equitability of the system in various configurations and watchlist volumes, including those falling within the HIOWC LFR Policy, SOP and use case.

While the report concluded that at the LFR System default face match threshold of 0.6, against a watchlist of 1,000 individuals, system performance for the metric of 'False-Positive Identification Rate' (FPIR), being the rate of incorrect recognition (i.e. false positives or false alerts) when subjects not on the watchlist pass through the zone of recognition, was 0.002 % or 1 in 60,000. When a watchlist of 10,000 individuals was ingested into the LFR system at the same threshold, however, the FPIR increased ten-fold to 0.017 % or 1 in 6000.

Efforts will be made to ensure that HIOWC watchlists are streamlined in so far as possible consistent with the purpose and will be limited to approx. less than 3,000.

The report also identified that at this threshold (0.6) there was, while not deemed statistically significant, differential in performance against different demographic groups with a higher True-Positive Identification Rate (TPIR) (the rate of successful recognition when subjects on the watchlist pass through the zone of recognition) in respect of Asian Females and the poorest for Black Females. A statistically significant difference in FPIR was present in different demographic groups at lower thresholds of 0.58.

The report did find a statistically significant differential in the TPIR in respect of age, finding that the LFR System performed better in relation to those aged 42 and over than those aged in the 20-41 age range, who are most likely to fall within the watchlist. Nevertheless, even for this age group this still delivered a TPIR of 89% and the report considered that the outcome was influenced by *"subject and environmental factors"* such as the individual's height and the density of the crowd in the LFR zone of recognition.

Notwithstanding that, and importantly for all data subjects, the report found that at face match threshold setting of 0.64, *"there were no false positive identifications, thus at this threshold the FPIR is identically 0.0 for all demographic groups".* HIOWC has therefore determined that 0.64 is the minimum threshold setting at which LFR is generally authorised to be deployed under the HIOWC LFR Policy and SOP.

While the report did report results of testing against two combined demographics, i.e. gender and ethnicity, it is not clear what additional impact the combination of age can have on the results. It is important to note that the testing which resulted in the report was conducted using appropriate quality recent custody style images, did not include categorise mixed race individuals separately, no testing of the impact of weather conditions took place, and subjects were instructed on how to behave in the zone of recognition. The report also identified more practical limitations of the system, such as that it performed worse for short subject, which in some cases could also denote a younger age, compared to a taller subject. HIOWC will continue, consistent with its obligations to process personal data fairly and lawfully and to carry out the PSED, to record and monitor the results of LFR Deployments in order to identify any adverse or unexpected impact of performance issues and consider what, if any, further mitigations are necessary.

- Explain how individuals will be made aware of the processing.

Several methods are proposed to make affected individuals, and the wider community, aware of the processing of personal data.

HIOWC already publishes a privacy notice which addresses its processing of personal data, including in connection with the processing of custody images etc. Those individuals who have already had contact with the police will be aware of the taking of their custody image and the processing of their personal data,

This is supplemented in relation to the deployment of LFR with the publication of an LFR specific privacy notice.

7 days in advance of all proposed deployments, HIOWC will issue an alert on its website and via social media. It is anticipated that this may be the subject of further coverage, for example in local print and broadcast media.

Where considered necessary and appropriate, as highlighted in the LFR Application and Authorisation, businesses and other organisations in the vicinity of the deployment will be engaged with both in advance and on the day.

LFR deployments will be overt. Appropriate signage will be placed at the perimeter of the LFR deployment location to ensure that individuals are alerted to the LFR deployment. These measures will be supplemented by officers and staff who are able to provide further information to members of the public, including leaflets on how to ascertain further information regarding the deployment and exercise any right of recourse. Individuals will be able to exercise a choice as to whether to enter the LFR deployment zone of recognition or seek to take steps to conceal their face.

Individuals who are flagged as a potential match which is then affirmed by the LFR Operator and LFR Engagement Officer and are the subject of an engagement will be proactively provided with an information leaflet on how to ascertain further information regarding the deployment and exercise any right of recourse.

To supplement the LFR Privacy Notice, HIOWC is also publishing other documentation pertaining to LFR to assist in advancing public understanding of the technology, its use and the compliance measures and safeguards that are in place.

- **Necessity**

HIOWC has identified several locations at which communities experience higher levels of serious violence and other priority crimes. HIOWC seeks to tackle this, with the support of ring-fenced Home Office funding, as part of Operation SENTINEL, which involves uniformed patrols being targeted toward these areas at specific times. Despite this, and the usual level of policing in place, there continues to be significant crime commission rates in the targeted locations, and it is proposed that these areas are included in the proposed LFR deployments locations.

In April 2024, HIOWC partnered with CrimeStoppers to launch a ‘Most Wanted’ gallery comprising 29 individuals wanted on warrant. As part of this campaign, CrimeStoppers attended various locations across the county, including in Basingstoke, Andover, Aldershot and Eastleigh, displaying the names and images of the individuals on digital advertising vans. HIOWC called on those individuals to hand themselves in to police, and members of the public could otherwise report them. Nevertheless, while this had

some success, despite this and other efforts, there remain multiple individuals wanted on warrant across the county. Having regard to the associated publicity, this could be considered more intrusive for the relevant individuals than the deployment of LFR. The intention is to continue to work in partnership with CrimeStoppers to maximise the effectiveness of wanted campaigns

Separately to these, HIOWC engages in Operation RELENTLESS in an effort to identify and reduce the number of outstanding suspects of crime and persons wanted on warrant across the constabulary. There continues to be significant numbers of individuals outstanding and the figures have since returned to levels even higher than at the start of the operation.

In relation to missing persons considered at increased risk of harm, the nature of these incidents is often such that locating the individual is an urgent priority given that they pose a risk to themselves and/or others.

Alternative approaches to LFR have therefore been tried but have failed to deliver the purposes.

As to whether other, less intrusive, measures might be available having regard to the resources available to HIOWC, even if more police officers/staff could be deployed in an effort to locate wanted individuals, suspects and/or persons considered at increased risk of harm, the use of LFR is in fact considered to be more likely to protect the rights of individuals given that there is a scientific basis for matching the biometric templates against the watchlist and this is then subject to multiple further human reviews, by the LFR Operator and the LFR Engagement Officer, each of whom has to be satisfied that the match is genuine.

- **Proportionality**

In relation to individuals wanted on warrant, for recall to prison, suspected of the commission of or otherwise under investigation for the commission of serious or priority offending, having regard to the law enforcement purpose(s) in respect of which there is considered to be a strong if not overwhelming public interest and a pressing social need, including the risk posed to the public and HIOWC's duties and tasks, when balanced against the rights of those individuals and taking into consideration the multiple safeguards in place, any interference with the rights of those individuals is considered to be proportionate to the aim pursued.

In relation to missing persons considered at increased risk of harm, the risk posed by those individuals to themselves and/or others and the need to safeguard them and the general public and ensure their wellbeing is considered to be proportionate to the objective.

The Court of Appeal in Bridges accepted the submission that, in relation to members of the public whose personal data was processed in the context of an LFR Deployment in so far as their image was captured by CCTV, a biometric extract was gleaned from it and which was sought to be matched against a watchlist and automatically and almost instantaneously deleted in the event of no potential match being flagged, the impact on their rights was *"negligible"* [143]. The LFR System cannot operate without processing

the personal data of such individuals, and therefore taking into account the negligible impact on their rights, the transparency measures and other safeguards in place and the minimal period for which the most sensitive personal data, in the form of the biometric template, is retained, the processing is considered to be proportionate to the pressing social need pursued.

- **Fairness**

HIOWC recognises that, as expounded by the Court of Appeal in Bridges, the overt deployment of LFR is (i) *"a novel technology"*, (ii) *"involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police"*, (iii) involves the processing of sensitive personal data, and (iv) involves automated processing.

It is also acknowledged that public understanding of the technology may be limited, and therefore the transparency and educational measures detailed above will be important in establishing the expectations of the general public as well as individuals affected by the LFR deployments (to whatever degree).

Consideration has been given to guidance given by regulators and concerns raised by civil society. In particular, regard has been had to the opinions issued by the Information Commissioner, including the opinion on 'The use of live facial recognition technology by law enforcement in public places' and subsequent opinion on 'The use of live facial recognition technology in public places'.

In order to ensure fairness, the efficacy and performance of the system has been considered together with scientific research on potential bias and/or discrimination in the system, in particular the NPL report. This is detailed elsewhere in this DPIA but has been used to determine the appropriate configuration for the system to eliminate any potential bias or discrimination.

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is incompatible with the original purpose:

The limited retention of biometric templates restricts their further use, whether for law enforcement or other purposes.

As set out above, in relation to custody or other police sourced images, it would be within the reasonable expectations of individuals that such personal data would be re-used for law enforcement purposes.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:

The HIOWC Policy and SOP introduce guidelines on the use of input images for LFR watchlists.

It is necessary to utilise images in order to obtain a biometric template.

While LFR does involve the processing of the personal data of multiple individuals who are not subject to inclusion a watchlist, the processing of the personal data of those individuals is necessary in order for potential matches to be identified and is strictly time limited to minimise any interference with their privacy, data protection and other rights.

The most intrusive data, the biometric templates, are deleted within 24 hours of an LFR Deployment even in the case of individuals who represent a potential match.

LFR logs and records that do not contain personal data are retained for 6 years.

Principle 4: Personal data must be accurate and kept up to date:

The importance of accurate and up to date reference image is identified in this DPIA and the HIOWC Policy and SOP include guidelines on the requirements for such images. Images of insufficient quality are rejected by the LFR System and will not be enrolled thereby further minimising the risk of inaccurate matches.

The accuracy of the LFR system itself has been the subject of scientific testing. The most recent NIST testing revealed that we note that in connection with the results of 1:N testing, for the purposes of investigation (which is intended to test law enforcement use cases by using the evaluation parameters to produce results for further human review to validate or dismiss returned candidates) the NEC algorithm nec_009 ranked 3rd out of 470 when tested using a frontal ‘mugshot’ (FNIR: 0.0011) and 4th out of 400 when testing using a profile ‘mugshot’ (FNIR: 0.0803) and 1st out of 430 using a webcam mugshot (FNIR: 0.0071). The results of NPL testing are detailed elsewhere in this DPIA.

Measures are in place to carry out ongoing review and governance of the accuracy, efficacy, equitability and general performance of the LFR system. This includes considering a range of metrics, such as the number of faces seen, the number of alerts, the number of false matches including the False Positive Identification Rate/False Alert Rate and the number of false matches as a proportion of the total number of matches, the number of engagements, the number of arrests/disposals, as well as wider considerations, such as on overall crime figures and the impact on public confidence.

At the authorised threshold configuration for general LFR deployments, it anticipated that the False Positive Identification Rate will be zero having regard to the NPL research and deployments by other forces at the same configuration. It is acknowledged that by prioritising the minimisation/extinguishment of false alerts and maximising equitability, the efficacy of the LFR system in making positive identifications may be diminished.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

A specified retention policy pertaining to HIOWC's LFR Deployments has been developed and shall apply.

In relation to custody images imported into the LFR system as part of watchlist, only those images which are lawfully held by the police will be utilised.

Custody images will be extracted by HIOWC systems and saved to an encrypted USB memory stick under the control of the LFR Deployment silver commander. This will be undertaken no longer than 24 hours prior to the deployment.

The watchlist images will be ingested into the LFR system as part of the deployment, which will allow a biometric template of those images to be created. This will be retained throughout the course of the deployment but will be deleted from the LFR system by no later than 24 hours following the conclusion of the deployment.

CCTV images obtained as part of the deployment will be retained for a minimum of 31 days, but may be retained for a longer period where required, for example in the event of a complaint or where relevant to an investigation or prosecution.

Biometric templates drawn from CCTV images which do not result in a potential match being flagged are deleted from the LFR system automatically and almost instantaneously.

Biometric templates drawn from CCTV images which result in a potential match being flagged will be deleted by no later than 24 hours following the conclusion of the deployment.

Deployment logs containing personal data will be retained as soon as possible but within 31 days at the latest:

- Deployment Record to allow a review of the whole deployment.
- Match Report to allow secondary, retrospective review of any matches flagged by the LFR system and subsequent engagements.

Deployment logs that do not contain personal data will be retained for 6 years.

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:

HIOWC is required to take appropriate technical and organisational measures in respect of personal data which it processes. The LFR System is subject to the following security measures:

Technical:

- The application is non-networked and non-configured to extend to the cellular network as an additional geographical protection.

- The LFR application is ‘closed’ and not connected to other HIOWC systems or the internet.
- The HIOWC watchlist is downloaded from the HIOWC crime recording system by specific officers/encrypted USB identified for use on the closed LFR system
- The dashboard and RESTful API are secured with SSL and TLS by default.
- All connections are directed through HTTPS.
- The LFR application can be connected to mobile devices using a private access point with three levels of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App.

Organisational:

- Two types of access will be available to the application – ‘user’ and ‘administrator’ access levels.
- Each LFR Operator will be given a username and password which they will be forced to change on initial use of the application (‘Active Directory’ strength of eight characters to include upper and lower case as well as being alpha numeric.
- Passwords are security protected.
- LFR System operating staff will have police vetting clearance to a minimum of Management Vetting / Security Clearance level.
- Role- based access controls.
- LFR System access is only granted to users following completion of training.
- The LFR system is staffed when in use and therefore physical protections are in place.
- Deployment data stored on the system is securely wiped following each deployment.
- As a contingency against the LFR system technology failing and requiring the LFR Operator to wipe and reset it the encrypted USB is retained with the LRF Operator under the end of the Deployment meaning that they are able to reimport the watchlist to the rebooted LFR application enabling the deployment to continue.
- The physical encrypted USB remains the responsibility of the HIOWC LFR Silver Commander during the LFR deployments.

Audit:

- The LFR System has an inbuilt and robust audit file log CSV file (hashed).
- Audit data enables ‘logging data’ to be retained regarding user activity that enables user and system auditing to be conducted.

In relation to HIOWC Joint Operations Unit officers and staff, these individuals will have been subject to appropriate police vetting and are subject to obligations of confidentiality and have received general data protection and information security training as well as LFR specific training.

7. Personal data will be processed in accordance with the individual’s data protection rights:

HIOWC already publishes a privacy notice which details individuals' data protection rights including providing details of the Data Protection Officer (DPO) and rights of recourse.

In relation to HIOWC's LFR deployments, a specific supplementary privacy notice has been prepared and published providing further detail of the specific application of these rights. This is not only made generally available online, but will be highlighted to individuals at the perimeter of the zone of recognition of HIOWC LFR deployments, for example through dedicated officers who can explain, provide information and direct individuals to the notice, a QR code directing individuals to the notice etc. Furthermore, for those individuals who are engaged with by an Engagement Officer further to a potential watchlist match being flagged by the LFR System, HIOWC LFR Policy and SOP require those individuals to be pro-actively offered information about their rights and mechanisms to seek recourse.

A dedicated email account for complaints and communications relating to LFR has been adopted, but this supplements rather than replaces existing channels and individuals can still contact the DPO.

Complaints and concerns will form part of the ongoing review and oversight arrangements for HIOWC LFR deployments.

In addition, the briefing to all officers and staff engaged in HIOWC LFR deployments will emphasise that in the event of any perceived infringement of the rights of individuals or failure to comply with the requirements of the HIOWC LFR documentation, this should be reported to the Silver Commander who will record the incident with a view to complying with section 81 Data Protection Act 2018, but may also be reported to the Chief Constable and/or the Information Commissioner.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:

The Data Protection Act 2018 restricts the transfer of personal data processed for law enforcement purposes outside the UK and the UK GDPR imposes safeguards on the transfer of personal data to countries which fail to provide adequate protections for personal data.

The LFR System is a stand-alone, non-networked, on premise application, which does not involve the transfer of personal data outside of the UK.

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & UK GDPR:

As data controller in respect of HIOWC LFR deployments, HIOWC is responsible for the processing of personal data. The HIOWC LFR Documentation demonstrates HIOWC's commitment to complying with its legal and regulatory obligations and best practice in securing data protection compliance.

Logging and other records required to be created relating to HIOWC LFR watchlists and LFR deployments will enable the review and auditing of processing activities internally and the update of HIOWC LFR documentation as required.

In addition, the briefing to all officers and staff engaged in HIOWC LFR deployments will emphasise that in the event of any perceived infringement of the rights of individuals or failure to comply with the requirements of the HIOWC LFR documentation, this should be reported to the Silver Commander who will record the incident with a view to complying with section 81 Data Protection Act 2018, but may also be reported to the Chief Constable and/or the Information Commissioner.

This LFR system and HIOWC LFR documentation will also be subject to ongoing external periodic review and oversight. The PCC for HIOWC ultimately has oversight of policing within HIOWC. It is proposed that consultation with relevant groups will continue, including to consider the results of HIOWC LFR deployments.

5. Identifying and assessing risks

Actions required to fill further data compliance gaps:

Where a data protection compliance gap has been identified and there is no pre-planned activity to address it in the above table in 5a), then they will need to be recorded as risks in the below table.

The main focus of the risk assessment within the DPIA is to consider the **risks to the interests of the individuals** whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

However, although not detailed below in the risk table, non-compliance with the legislation will have a detrimental impact on the organisation resulting in additional scrutiny from the Information Commissioner's Office and the potential to receive significant fines.

The below listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will need to be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

	Describe the problem that is the risk, the vulnerability that creates the problem and the potential impact on individuals. Focus mainly on the impact on the data subject. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, some impact, or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.

1	The compilation of watchlists is based on inaccurate or out of date information.	Possible	Severe	Medium	The HIOWC LFR Policy and SOP require that watchlists are confirmed no longer than 24 hours prior to a deployment to ensure that the available information is as up to date as possible. Nevertheless, there is a residual risk that information could change between the confirmation of the list and the deployment. Engagement officers will be specially trained to ensure that any engagement with individuals is appropriate and lawful and all individuals who are engaged with will be provided with information regarding the rights and route of recourse.	LFR Silver Commander – routine deployment activity. Engagement Officers – routine deployment activity.	Low
2	Images used to extract biometric templates in respect of individuals included on watchlists are of insufficient quality or out of date.	Possible	Severe	Medium	The HIOWC LFR Policy and SOP state that in the first instance preference should be given to using police-originated images, i.e. custody images, which are of sufficient quality (confirming to the NPIA '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)') and are sufficiently		Low

					recent to bear a likeness to the individual. Where this is not possible, consideration may be given to the use of outdated, third-party originated and/or lesser quality images [subject to safeguards]. The LFR system will not create and load a biometric template from any images of insufficient quality. Specific measures are in place requiring that the anticipated likelihood of individual's under the age of 18, individual with a disability or individual subject to gender reassignment treatment, being groups which may be more likely to be affected by image quality/sufficiency, are flagged in the LFR application to the Authorising Officer. Measures are in place to ensure that officers involved in the deployment are made aware to take this into account in considering specific potential matches and exercising their discretion.	Automated LFR system functionality. LFR Silver Commander – routine deployment activity.	
3	Images used to extract biometric templates in	Probable	Severe	Medium	It is acknowledged that concerns have been raised by the Biometrics		Low

	respect of individuals included on watchlists are held unlawfully by HIOWC				and Surveillance Camera Commissioner as to the inability of policing to carry out bulk data deletion from police systems potentially resulting in the indefinite retention of personal data including custody images in circumstances where this may fall outside retention periods or otherwise be justifiable. In order to mitigate this risk, technical measures in place to ensure that images identified and extracted for inclusion are lawfully held as required by the HIOWC LFR SOP.	Strategic LFR Lead – routine deployment measure	
4	Children or vulnerable individuals are proposed to be included on watchlists without them being flagged to authorising officers and/or to deployment commander.	Possible	Severe	Medium	The HIOWC LFR Policy and SOP require that the proposed inclusion of individuals aged under 13, aged 13-18 and/or known to have a disability in the watchlist are highlighted to the Authorising Officer in the LFR Application to ensure that specific consideration is given to the necessity and proportionality of their inclusion in the Watchlist and any additional safeguards which may be required can be implemented.	LFR Silver Commander & Authorisation Officer – routine deployment activity.	Low
5	Individuals are unaware of the processing of their	Possible	Some impact	Medium	HIOWC already makes available an overarching privacy notice/privacy policy which is published online and		Low

	personal data in the course of LFR deployments.				is thereby accessible to data subjects. The HIOWC LFR Policy and SOP require that any proposed deployment be advertised on the HIOWC website and on social media 7 days prior to the deployment. It is anticipated that this will then result in further coverage, including in traditional news media at a local level. The Policy and SOP further require that any LFR deployment be conducted overtly, and with appropriate signage outside the zone of recognition to alert the public to the deployment prior to entering. This will be supplemented by officers on the ground who will be able to assist members of the public by providing information, including leaflets, in relation to the deployment. The Policy and SOP require that any individual who is engaged with as a result of a potential match is pro-actively offered a copy of a leaflet directing them to further information,	LFR Team via HIOWC Head of Communications LFR Silver Commander – routine deployment activity. Engagement Officers – routine deployment activity.	

					including in relation to their rights and recourse mechanisms. An LFR specific privacy notice is published providing more detailed information regarding the use of LFR by HIOWC.	Senior Information Governance Manager	
6	Individuals are unaware of their data protection rights and recourse in respect of the processing of their personal data.	Probable	Some impact	Medium	HIOWC already makes available an overarching privacy notice/privacy policy which is published online and is thereby accessible to data subjects. An LFR specific privacy notice is also published providing more detailed information regarding the use of LFR by HIOWC. The Policy and SOP further require that any LFR deployment be conducted overtly, and with appropriate signage outside the zone of recognition to alert the public to the deployment prior to entering. This will be supplemented by officers on the ground who will be able to assist members of the public by providing information, including leaflets, in relation to the deployment. The Policy and SOP require that any individual who is engaged with as a	Senior Information Governance Manager LFR Silver Commander – routine deployment activity. Engagement Officers –	Low

					result of a potential match is pro-actively offered a copy of a leaflet directing them to further information, including in relation to their rights and recourse mechanisms.	routine deployment activity.	
7	The personal data of innocent individuals is gathered by police	Probable	Minimal	Medium	The operation of LFR necessarily involves the processing of the personal data, including biometric data, not only of individuals captured on a watchlist, but also members of the public who happen to be in the deployment location and who are not themselves of legitimate interest to the police. The processing is, however, minimised and subject to safeguards. While processing involves the capture of CCTV images and the automated extraction from those images of a biometric template for comparison against the watchlist, where no potential match is identified at the applicable configuration, the biometric template of the member of the public is automatically and almost instantaneously deleted and data retention policies and procedures apply to related personal data to ensure that the processing is minimised to what is strictly	Automated LFR System functionality.	Low

					necessary to enable the law enforcement purposes to be carried out and to support individuals' rights of recourse. The interference with the rights of members of the public is therefore limited. LFR deployments are overt, publicised in advance, have a dedicated published privacy notice, subject to transparency measures at the perimeter of the deployment location enabling individuals to choose not to enter the LFR zone of recognition or to seek to take counter-measures, and staffed with officers who can provide further information including details of how to seek recourse. This is in addition to the approval and governance process for the use of LFR as detailed across the suite of HIOWC LFR documentation.		
8	CCTV images are retained for longer than is necessary.	Possible	Some impact	Medium	HIOWC has established a retention policy in connection with the deployment of LFR which is reflected in the HIOWC LFR Policy, SOP, LFR Appropriate Policy Document and LFR Privacy Notice.	Strategic LFR Lead	Low

					The CCTV images will be deleted after 31 days. On limited occasions when it is necessary to retain any specific sections of footage longer for a criminal investigation or to investigate a complaint.	LFR Team - ongoing part of post deployment activity	
9	CCTV images are stored insecurely.	Possible	Some impact	Medium	The LFR system is a stand-alone non-networked system, which is subject to security measures, including: the LFR application has two layers of password protection to access the application; the LFR application is staffed when in use and therefore physical protections are in place; LFR system engineers are deployed with the system when in operation; deployment data stored on the system is securely wiped following each deployment; individual users of the LFR application and subject to role based access controls with limited user permissions; the dashboard and RESTful API are secured with SSL and TLS by default, and all connections are directed through HTTPS; the LFR application can be connected to mobile devices using a private access point with three levels	LFR Operator - routine deployment activity.	Low

					of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App; and, logging data is retained of user which enables auditing to be conducted. CCTV is retained on police systems for a minimum of 31 days post-deployment and longer where required and is subject to MOPI.		
10	Biometric templates are retained for longer than is necessary.	Possible	Some impact	Medium	HIOWC has established a retention policy in connection with the deployment of LFR which is reflected in the HIOWC LFR Appropriate Policy Document, SOP and Privacy Notice. The biometric templates of images used for LFR are automatically deleted by the LFR system within 24 hours of the conclusion of the deployment and automatically and instantaneously when the person passing through the recognition zone does not match a person on the watchlist.	Strategic LFR Lead Automated LFR system functionality.	
11	Biometric templates are stored insecurely.	Possible	Some impact	Medium	The LFR system is a stand-alone non-networked system, which is subject to security measures, including: the LFR application has	Automated LFR System functionality.	Low

					two layers of password protection to access the application; the LFR application is staffed when in use and therefore physical protections are in place; LFR system engineers are deployed with the system when in operation; deployment data stored on the system is securely wiped following each deployment; individual users of the LFR application and subject to role based access controls with limited user permissions; the Dashboard and RESTful API are secured with SSL and TLS by default, and all connections are directed through HTTPS; the LFR application can be connected to mobile devices using a private access point with three levels of protection comprising specific IP addressing, password access to the access point, and password access to the mobile App; and, logging data is retained of user activity in accordance with section 62 Data Protection Act 2018 which enables auditing to be conducted.	LFR Operator – routine deployment activity LFR Operator - routine deployment activity. Automated LFR functionality.	
12	Biometric templates are used for purposes other than the specified purpose.	Possible	Some impact	Medium	Data protection law regulates and restricts the further processing of personal data, as provided by s.36(3) Data Protection Act 2018		Low

					which prevents further processing for non-law enforcement purposes unless authorised by law and requires any further processing for law enforcement purposes to be authorised by law, necessary and proportionate. The fairness of such processing is further limited by the scope of the HIOWC LFR specific privacy notice/policy. In relation to the biometric templates of members of the public, this data is automatically and almost instantaneously deleted by the LFR system where no match is identified thus preventing their retention and further use. In relation to the biometric templates of individuals on the watchlist and individuals in respect of whom a potential match is flagged, these biometric templates are deleted no later than 24 hours following the end of the deployment. In practice, there are therefore very limited opportunities for biometric templates to be used for any other purpose. Any proposal to do so is required to be subject to specific	Automated LFR system functionality. LFR Operator – routine deployment activity.	

					legal advice and input from the HIOWC DPO.		
13	CCTV images are used for purposes other than the specified purpose.	Possible	Some impact	Medium	Data protection law regulates and restricts the further processing of personal data, as provided by s.36(3) Data Protection Act 2018 which prevents further processing for non-law enforcement purposes unless authorised by law and requires any further processing for law enforcement purposes to be authorised by law, necessary and proportionate. The fairness of such processing is further limited by the scope of the HIOWC LFR specific privacy notice/policy. Any proposal to do so is required to be subject to specific legal advice and input from the HIOWC DPO.		Low
14	Personal data, in particular watchlist images, are transferred/stored insecurely between HIOWC and LFR systems	Possible	Some impact	Medium	Watchlist images are saved from HIOWC systems to an encrypted USB memory stick under the control of the Deployment Silver Commander. The time period during which personal data is stored on the encrypted USB memory stick is minimised by the only being saved no more than 24 hours prior to the deployment and required to be wiped	LFR Silver Commander – routine deployment activity.	Low

					within a further 24 hours of the deployment.		
15	Training of LFR system involves the unlawful processing of personal data.	Possible	Severe	Medium	HIOWC is not a data controller in respect of, and is therefore not legally responsible for, the processing of personal data to train the LFR system being deployed; this is the role of the supplier. Nevertheless, HIOWC is concerned to ensure that the LFR system is trained in such a way that its outcomes are suitable for the purpose and do not result in false matches being flagged or in particular demographic groups or individuals displaying protected characteristics being exposed to a greater risk of a false match being flagged. HIOWC has reviewed the published scientific research on the specific LFR system to be deployed and the HIOWC Policy and SOP explicitly identify the configurations at which the system may be deployed to ensure that any risk of false matches or discrimination is minimised or extinguished.	Strategic LFR Lead – complete but reviewed regularly.	Low

16	LFR system results in greater false matches being flagged against individuals within certain demographics/of certain protected characteristics, potentially exposing individuals to the risk of engagement.	Possible	Severe	Medium	HIOWC has reviewed the published scientific research on the specific LFR system to be deployed and the HIOWC Policy and SOP explicitly identify the configurations at which the system may be deployed to ensure that any risk of false matches or discrimination is minimised or extinguished.	Strategic LFR Lead – reviewed regularly.	
17	LFR system operator fails to exercise own judgement in respect of match flagged by LFR system.	Possible	Severe	Medium	HIOWC Policy and SOP require that officers and staff involved in an LFR Deployment must receive LFR training prior to being deployed, and LFR operators receive specialist training including in relation to the operation of the system, environmental and other factors which may inhibit its effectiveness and their role in exercising independent judgement in relation to the flagging of potential matches. In addition, prior to every deployment, officers and staff engaged in the Deployment are briefed including to highlight any specific risks. An LFR Operator's affirmation of a flagged potential match is not final, however, as LFR Engagement Officers also have to affirm the	LFR Silver Commander – routine deployment activity.	Low

					match on the ground prior to effecting an engagement. In practice, it is anticipated that the use of a biometric template to produce a potential match in circumstances where this is then supported by both the LFR Operator and LFR Engagement Officer will result in more accurate outcomes than human input alone. Both LFR Operator logs and system logs are maintained in order to enable post-deployment reviews and audits to be carried out which would serve to identify concerns that LFR Operators are overly reliant on flagged potential matches, which would dictate that further training be undertaken and may call for additional oversight to be established.	Engagement Officers – routine deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	
18	LFR system operator wrongly affirms match flagged by LFR system.	Possible	Severe	Medium	HIOWC Policy and SOP require that officers and staff involved in an LFR deployment must receive LFR training prior to being deployed, and LFR operators receive specialist training including in relation to the operation of the system, environmental and other factors	LFR Silver Commander – routine deployment activity.	Low

					which may inhibit its effectiveness and their role in exercising independent judgement in relation to the flagging of potential matches. In addition, prior to every Deployment, officers and staff engaged in the Deployment are briefed including to highlight any specific risks. An LFR Operator's affirmation of a flagged potential match is not final, however, as LFR Engagement Officers also have to affirm the match on the ground prior to effecting an engagement. In practice, it is anticipated that the use of a biometric template to produce a potential match in circumstances where this is then supported by both the LFR Operator and LFR Engagement Officer will result in more accurate outcomes than human input alone. Both LFR Operator logs and system logs are maintained in order to enable post-Deployment reviews and audits to be carried out which would serve to identify concerns that LFR Operators are overly reliant on flagged potential matches, which	Engagement Officer – routine deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	

					would dictate that further training be undertaken and may call for additional oversight to be established.		
19	Engagement officer fails to exercise own judgement in respect of match flagged by LFR system.	Possible	Severe	Medium	The LFR Engagement Officer provides the third element of confirmation prior to engagement, based first on the LFR system flagging a potential match in a biometric template, which must then be affirmed by the LFR Operator and finally the LFR Engagement Officer. HIOWC LFR Policy and SOP require that officers and staff involved in an LFR deployment must receive LFR training prior to being deployed, and LFR Engagement Officers receive specialist training on their role. In addition, prior to every deployment, officers and staff engaged in the Deployment are briefed including to highlight any specific risks. In practice, it is anticipated that the use of a biometric template to produce a potential match in circumstances where this is then supported by both the LFR Operator and LFR Engagement Officer will	LFR Operator & Engagement Officers – routine deployment activity. LFR Silver Commander – routine deployment activity.	Low

					result in more accurate outcomes than human input alone. Both LFR Operator logs and system logs are maintained in order to enable post-deployment reviews and audits to be carried out which would serve to identify concerns that LFR Engagement Officers are overly reliant on flagged potential matches and the view of LFR Operators and are failing to exercise their own independent judgement, which would dictate that further training be undertaken and may call for additional oversight to be established.	LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	
20	Engagement officer wrongly affirms match flagged by LFR system.	Possible	Severe	Medium	The LFR Engagement Officer provides the second element of confirmation prior to engagement, based first on the LFR system flagging a potential match in a biometric template, which must then be affirmed by the LFR Operator and finally the LFR Engagement Officer. HIOWC LFR Policy and SOP require that officers and staff involved in an LFR Deployment must receive LFR training prior to being deployed, and LFR Engagement Officers receive specialist training on their role. In	LFR Operator & Engagement Officers – routine deployment activity. LFR Lead & LFR Silver Commander – routine deployment activity.	Low

					addition, prior to every Deployment, officers and staff engaged in the Deployment are briefed including to highlight any specific risks. In practice, it is anticipated that the use of a biometric template to produce a potential match in circumstances where this is then supported by both the LFR Operator and LFR Engagement Officer will result in more accurate outcomes than human input alone. In the event that an LFR Engagement Officer wrongly affirms a potential match and engages with an individual, not only are LFR Engagement Officers trained in their role and expected to engage the public in a respectful manner, but it is a requirement that they offer individuals information regarding their rights, including a mechanism to seek redress. Both LFR Operator logs and system logs are maintained in order to enable post-deployment reviews and audits to be carried out which would serve to identify concerns that LFR	LFR Silver Commander & Strategic LFR Lead – routine	

					Engagement Officers are overly reliant on flagged potential matches and the view of LFR Operators and are failing to exercise their own independent judgement, which would dictate that further training be undertaken and may call for additional oversight to be established. All officers and staff engaged in HIOWC LFR Deployments are briefed that in the event of any perceived infringement of the rights of individuals or failure to comply with the requirements of the HIOWC LFR Documentation, this should be reported to the Silver Commander who will record the incident with a view to complying with section 81 Data Protection Act 2018, but may also be reported to the Chief Constable and/or the Information Commissioner.	deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	
21	Individual engaged on basis of false match.	Possible	Severe	Medium	LFR systems involve a scientific approach to identifying an individual which is then overlaid by the safeguards of requiring an LFR Operator to review and affirm a potential match, which is then further verified by the LFR Engagement		Low

					Officer before any action is taken against the individual. LFR Engagement Officers will then seek to confirm the individual's identity and are trained in dealing with the public professionally and courteously. The mere fact that the LFR System has flagged a potential match does not automatically result in a match being considered confirmed and nor does it automatically lead to action, such as arrest, being taken against an individual. Police officers and staff have a critical role in the process and over-ride the LFR system. Both LFR Operator logs and system logs are maintained in order to enable post-deployment reviews and audits to be carried out which would serve to identify concerns that LFR Engagement Officers are overly reliant on flagged potential matches and the view of LFR Operators and are failing to exercise their own independent judgement, which would dictate that further training be undertaken and may call for additional oversight to be established.	Engagement Officers - routine deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	

					Any individual who is the subject of a false match and is then engaged with is required to be offered a leaflet regarding the LFR deployment and directing them to information regarding their rights and recourse. All officers and staff engaged in HIOWC LFR Deployments are briefed that in the event of any perceived infringement of the rights of individuals or failure to comply with the requirements of the HIOWC LFR Documentation, this should be reported to the Silver Commander who will record the incident with a view to complying with section 81 Data Protection Act 2018, but may also be reported to the Chief Constable and/or the Information Commissioner.	Engagement Officers - routine deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	
22	False match results in over-retention of personal data	Possible	Severe	Medium	Where the LFR system identifies a potential match which is not affirmed by the LFR Operator or LFR Engagement Officers, i.e. a false match, while this would mean that the biometric template relating to that individual is retained for a longer period than where no match is identified, in which case the biometric template would be deleted		Low

					almost immediately, the retention of such data is nevertheless minimised with such data only being retained for up to 24 hours post-deployment thus minimising any adverse impact and inhibiting the use of such data for other unauthorised purposes. All officers and staff engaged in HIOWC LFR Deployments are briefed that in the event of any perceived infringement of the rights of individuals or failure to comply with the requirements of the HIOWC LFR Documentation, this should be reported to the Silver Commander who will record the incident with a view to complying with section 81 Data Protection Act 2018, but may also be reported to the Chief Constable and/or the Information Commissioner.	LFR Operator – routine deployment activity. LFR Silver Commander & Strategic LFR Lead – routine deployment activity.	
23	Individual affected by LFR unsure of how to exercise their data subject rights.	Possible	Some impact	Medium	In addition to the HIOWC published privacy notice, which details how individuals can exercise their data rights, an LFR specific privacy notice has been published, transparency information is made available at the perimeter of the LFR zone of recognition and individuals who are the subject of an engagement are required to be offered information on	LFR Team	Low

					their rights including mechanisms for seeking redress.		

**If you have accepted any of the above risks <u>without</u> taking any risk reducing action you must provide a rationale for doing so in the 'Agreed Actions' column.*

6. Authorisation of DPIA:

DPIA2 copies will be retained by the Information Governance Team in the Joint Information Management Unit (JIMU) and within the relevant Project Management records.

a) Approval signatories

Item	Name / role / date	Notes
Risk Reducing Measures approved by **Information Asset Owner:**	C/Supt. Tim Rowlandson (LFR) 08/12/2025 *Tim Rowlandson* Tom Kempster (RMS) - 09/12/2025 *Tom Kempster*	Acceptance of residual risk level and integration of any BAU actions
Residual risks approved by project **Senior Responsible Officer**:	ACC Paul Bartolomeo – 09/12/2025 *Paul Bartolomeo*	Acceptance of mitigating actions and completion date. Integration into project plan.
Data Protection Officer approval of DPIA:	Jason Saxon – Director of Data and Information 09/12/2025 *Jason Saxon*	Approval of residual risk and processing to proceed.
DPO advice (by exception):		

Distribution List	**Distribution List**	
Name	**Force**	**LFR & DPIA Involvement**
Jason Saxon	HIOWC	Data Protection Officer & Director of Data and Information & DPIA Signatory
Detective Chief Superintendent Tim Rowlandson Tom Kempster	HIOWC HIOWC	Information Asset Owner Strategic LFR Lead & DPIA action owner & DPIA Signatories
ACC Paul Bartolomeo	HIOWC	Senior Responsible Officer & DPIA Signatory
Abbie Newnham	HIOWC	Project Manager
D/Supt. Gabe Snuggs	HIOWC	Authorising Officer
Tim Rowlandson (Strategic LFR Lead)	HIOWC	Strategic LFR Lead & DPIA action owner

James Sullivan	HIOWC (JOU)	LFR Silver Commander for 18/12/25 deployment & DPIA action owner
Sharon Warwick	HIOWC	Senior Information Governance Manager &

b) Residual high risks (complete only if there are any 'high' residual risks):

Item	Decision / Name / role / date	Notes
SIRO decision on referring to ICO:	N/A no high residual risks	If not referring to ICO SIRO to record rationale
SIRO Rationale:		
Date and name of person referring DPIA to ICO:		As required by law if any high residual risks remain.
Summary of ICO advice:		

c) Accountability – update of governance records and 'records of processing':

Accountability Task	IGO to date & sign when task complete	IGM to date & sign when checked complete
Information Asset Register updated	05/12/2025	Senior Information Governance Officer
Privacy Notice reviewed to see if new processing needs adding.	LFR Specific Privacy Notice produced and published on HIOWC website (LFR Page) 02/09/2025	Checked 09/09/2025 & 03/12/2025 - Senior Information Governance Manager
Trigger points for action tracking agreed and in DPIA Register	No outstanding actions	N/A
ISA Catalogue / DPC Register updated if any new ISAs / DPCs.	Added 01/09/2025	Checked 09/09/2024 & 03/12/2025 - Senior Information Governance Manager

7. Review / Update of DPIA:

a) Record Of Review

Review Date	Reviewing IGO	Reason for Review
		Add delete as appropriate list *i. 1 Year from sign-off* *ii. Data Guardian January Review* *iii. Exception criteria (please state which one)*
Record: Has the scope and nature of the processing changed? (Detail yes or no below)		
Ask the DG: 1. Scenarios in which they use the system? Have they changed or increased? 2 Has the way in which you use the system or the amount / type of data you put in the system changed significantly? 3. Ask about the compliance gaps and actions focused within the DPIA2. *What were the changes in the scope of the processing / how does this change affect DP compliance / any new risks or mitigating actions that have been agreed. List in table below.*		
Record: Has there been any changes to data protection legislation that affects compliance / risks / mitigations? (If yes detail below)		
No. Or if yes – state what the legislative change is and the impact of the change		
Record whether the DG is happy that the risks continue to be sufficiently mitigated? (If no detail below)		
If they are sufficiently mitigated record, "DG satisfied with residual risks". If not, then record why not.		

Please Note: If there are any new risks / actions or any changes to existing ones must be captured in risk table below:

b) Changes to Data Protection Risks and Actions

	Describe the problem that is the risk, the vulnerability that creates the problem and the potential impact on individuals. .	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, some impact or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date**	**Residual Risk score** Low, high or medium.

c) Review Sign Off

DPIA Review - Signatories	**Name / role / date**	**Notes**
Information Asset Owner or Data Guardian.		IG will advise on correct signatories according to DPIA review guidance document
JIMU (IGO, IGM or DPO)		IG will advise on correct signatories according to DPIA review guidance document
DPO advice (by exception):		

d) IG Checklist

DPIA Review Checklist	Date	Signature
Next DPIA Review Date		
DPIA Register Updated		
IAR Register updated (if applicable)		