Specific Appropriate Policy Document: Live Facial Recognition

INTRODUCTION

This Live Facial Recognition (LFR) specific Appropriate Policy Document (APD) has been produced in accordance with Hampshire and Isle of Wight Constabulary's' (HIOWC) obligations under Part 3 of the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). It should be read alongside the HIOWC LFR specific Privacy Notice and the HIOWC general Privacy Notice. The Data Protection policy specific to LFR can also be found in the LFR Policy and Data Protection Impact Assessment (DPIA).

THIS POLICY DOCUMENT

Sections 35(3), 35(5)(c) and 42 in Part 3 of the DPA 2018 set out the requirement for an APD to be in place when conducting sensitive processing for Law Enforcement (LE) purposes. Schedule 1, Part 4 of the DPA 2018 sets out the requirement for an APD to be in place when processing special category data under the UK GDPR.

Sensitive processing is defined in Part 3 section 35(8) DPA 2018 and is equivalent to UK GDPR Article 9(1) special category data. It includes:

a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual's sex life or sexual orientation.

This APD will satisfy those requirements and demonstrate how HIOWC meets the provisions set out in the 'data protection principles' within section 34 of the DPA 2018 and Article 5 of the UK GDPR.

DESCRIPTION OF DATA PROCESSED

The HIOWC 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.

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined 'watchlist' in order to locate persons of interest by generating an alert when a possible match is found.

Biometric data used to uniquely identify an individual is considered to constitute sensitive processing when used for law enforcement purposes / special category personal data. The sensitive processing / special category data processed utilising LFR is the biometric facial template data, created from images of individuals faces, for the purpose of uniquely identifying an individual together with the input and CCTV images in so far as they are capable of revealing racial or ethnic origin and/or religious beliefs.

The watchlist for LFR will usually be comprised of a copy of a subset of the HIOWC custody image dataset but may also include other lawfully held images. These custody images have been previously collected by HIOWC when an individual has been arrested and detained. All watchlist images will have a biometric template created at the point of enrolment to the LFR system.

All images of faces collected via the live LFR cameras will have a biometric facial template created for comparison against the biometric facial templates of persons on the watchlist.

Where the comparison of the LFR live camera images does not generate an alert of a potential match against an image on the watchlist, the biometric template will not be further processed and biometric data of the individual will be automatically and permanently deleted once this comparison has been completed, which is an almost instantaneous process. No other personal identifiers are collected from the live cameras in addition to the image and biometric template.

HIOWC will use LFR technology for the following policing objectives:

a) For the purpose of locating 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) For the purpose of locating individuals who are designated as a current 'missing person considered at increased risk of harm' that HIOWC has assessed 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) For the purpose of locating 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.

Statistical research and analysis may be carried out to analyse and develop the accuracy, efficacy and equitability of HIOWC's use of LFR systems. Any processing of images and

biometric templates via LFR for this reason would not involve the need to identify or locate persons. Such research would be subject to the additional safeguards required in section 19 of the DPA 2018 and Article 89 of the UK GDPR, such as pseudonymisation and appropriate technical security measures.

PROCEDURES FOR ENSURING COMPLIANCE WITH THE DPA & UK GDPR PRINCIPLES

1) Principle (1): lawfulness, fairness and transparency

The processing of personal data for LFR must be lawful and fair when used for the 'law enforcement' purpose, under the provisions of the Part 3 of the DPA 2018.

The processing of personal data LFR to locate missing persons who are at risk of, or pose a risk of, serious harm or to carry out any future research on the accuracy and efficacy of the use of LFR technology; will be subject to the provisions of the UK GDPR where processing of personal data for LFR must be lawful, fair and transparent.

HIOWC will satisfy the requirement of lawful, fair and transparent in the following ways:

Fairness & Transparency:

HIOWC will only use personal data for LFR in ways that citizens would reasonably expect and not use it in ways that have unjustified adverse effects on them. Citizens would expect HIOWC to use its available information and tactical capabilities to locate persons who evade court justice or prison recall, are a suspect of a criminal investigation for a range of specific offences or are missing persons considered at increased risk of harm

In order to ensure that citizens around the recognition zone are not surprised by the use of LFR, HIOWC will publicise its deployments of LFR at least 7 days in advance of any deployment on its website and social media channels. LFR signs will also be positioned ahead of any entry points into the recognition zone to make citizens fully aware of LFR use.

HIOWC is committed to ensuring transparency around its use of LFR by publishing, on its LFR webpage, the following documents: LFR specific Privacy Notice, LFR policy and procedures, Data Protection Impact Assessment, Legal Mandate, multiple impact assessments, advance notice of deployments and retrospective LFR deployment analysis.

Unjustified adverse effects of any inaccurate facial matching are mitigated by selecting a LFR system accuracy threshold setting of 0.64, where inaccurate system matches have been shown to be highly unlikely, and always having a police officer make the final decision about where a proposed facial match is believed to be the same person and whether to engage them.

Lawfulness:

In order for the use of LFR to satisfy 'lawful' it must not be inherently unlawful. A detailed description of how LFR is used lawfully, is documented in the HIOWC LFR Legal Mandate, the LFR Data Protection Impact Assessment, the LFR Human Rights Impact Assessment,

the LFR Equality Impact Assessment and the Surveillance Camera Assessment. In summary, compliance with the following key relevant laws underpins HIOWC's LFR lawfulness:

- Collection and future use of images taken during detention in police custody for the purposes of prevention and detection of crime, the investigation of offences or the conduct of prosecutions; is lawful under section 64A of the Police and Criminal Evidence Act 1984.

- HIOWC's use of information whilst using tactical policing capabilities (including LFR) for a 'policing purpose' falls within the scope of the Statutory Code of Practice on Police Information and Records Management (SCoP on PIRM): protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice and any other police duty or responsibility arising from common or statute law.

- As a public authority, HIOWC must comply with the provisions set out in the Human Rights Act (HRA) 1998. HIOWCs compliance with the protected rights and freedoms is set out in detail in the HIOWC LFR Human Rights Impact Assessment. In particular, citizens' right to respect for their private and family life, their home and their correspondence (Article 8, HRA 1998) as well as Article 14 (prohibition of discrimination in application of other rights) are of particular focus for any deployment of LFR and so HIOWC will ensure that following are satisfied:

    - It is in 'accordance with the law' (as set out in the LFR Legal Mandate). HIOWC is committed to ensuring its use of LFR is foreseeable to citizens by publishing, on its LFR website a comprehensive set of LFR documents so that they can understand how and when it will be used.
    - HIOWC's use of LFR will be 'necessary'. We will only deploy LFR where there is a supporting intelligence case suggesting it is an appropriate policing tool to use and where less privacy intrusive measures have been tried and have been unsuccessful or have been considered and believed that they would not be successful.
    - Any intrusion of citizen's privacy or other rights caused by LFR deployment will be carefully considered to ensure it is 'proportionate' to the policing purpose / objective of the deployment. Particular attention will be given to reducing privacy intrusion when deciding: watchlist curation, location of the LFR recognition zone, time and date of deployment and LFR system settings.

Lawful basis:

HIOWC must satisfy a lawful basis for processing personal data and special category data/conducting sensitive processing under whichever data protection laws the LFR processing is governed by (DPA 2018 or UK GDPR). The lawful bases HIOWC satisfies are set out as follows:

Lawful Bases for processing personal and sensitive / special category data for the law enforcement purpose (Part 3 DPA 2018):

a) Personal data:

The processing of personal data during the use or LFR will be necessary for the 'Law Enforcement' (LE) purpose, defined in section 31, as follows:

- Prevention, investigation, detection, prosecution of criminal offences;
- The execution of criminal penalties;
- The safeguarding against and the prevention of threats to public security.

HIOWC will use LFR specifically: to apprehend and prosecute offenders and prevent and detect criminal offences and safeguard public security. HIOWC will not rely on the consent of individuals to process their personal data for LFR purposes.

HIOWC's processing of personal data must also be 'authorised by law'. This is addressed more fully in the Legal Mandate but the police have a common law duty to protect life and property, bring offenders to justice and to prevent and detect crime. This is set out as the 'policing purpose' in SCoP on PIRM. This is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions.

b) Sensitive data:

HIOWC will not rely on individuals' consent for the processing of sensitive data during LFR and therefore section 35(5) requires us to satisfy a condition from Schedule 8 of the DPA 2018. HIOWC will satisfy one or more of the following conditions, dependent on the LFR deployment objective and curation of the watch list, and HIOWC has an Appropriate Policy document in place:

I. Statutory etc. purposes (Schedule 8(1)):

This is the primary condition relied upon and the condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

The police have a common law duty to protect life and property, bring offenders to justice and to prevent and detect crime, as identified by the 'policing purpose' in the SCoP PIRM. This is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions. Not only is the function itself in the substantial public interest, the processing connected with the use of LFR is necessary for reasons of substantial public interest where individuals included on the watchlist have not been identified through traditional policing methods but pose a risk to themselves or others.

The use of sensitive data in LFR processing will be strictly necessary as HIOWC will ensure that less intrusive measures have first been considered but are deemed unsuitable because they would compromise the policing purpose / objective. HIOWC will always balance the policing

purpose with the privacy interests of the individuals and the interests of the community to ensure the use of LFR remains proportionate.

This is the primary condition relied upon. However, there are other Schedule 8 conditions which may also apply:

II. Administration of justice (Schedule 8(2)):

This condition is met if the processing is necessary for the administration of justice.

E.g. The identification of individuals who are evading justice having committed a criminal offence or who are interfering with the administration of justice, such as being subject of a court warrant.

III. Vital Interests (Schedule 8(3)):

This condition is met if processing is necessary to protect the vital interests of the data subject or another individual, for example where a suspect poses a risk to the life of another.

IV. Safeguarding of children and of individuals at risk (Schedule 8(4)):

This condition is met in the below circumstances if consent cannot be given by the individual, cannot expect for it to be obtained or obtaining consent would prejudice the safeguarding purpose:

(a) the processing is necessary for the purposes of-
  (i) protecting an individual from neglect or physical, mental or emotional harm, or
  (ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is-
  (i) aged under 18, or
  (ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

E.g. processing of images which reveal racial or ethnic origin or religious beliefs or biometric data of persons believed to be missing persons where it is believed they could be at risk of neglect, physical, mental or emotional harm due to criminal offences; fulfilling the substantial public interest in locating them.

V. Personal data already in the public domain (Schedule 8(5))

This condition is met where processing relates to personal data manifestly made public by the data subject.

As the High Court recognised in NT1 & NT2 v Google LLC [2018] EWHC 799 (QB) at para.111 when considering an equivalent provision, for data to fall within the scope of this condition "does not require a deliberate decision or "step" by the data subject "to make" the information public, but rather (a) the taking by him of a deliberate step or steps, as a result of which (b) the information is "made public". A person who deliberately conducts himself in a criminal fashion runs the risk of apprehension, prosecution, trial, conviction, and sentence" and the processing of images and other personal data pertaining to the individual is the ordinary consequence of such action.

VI. Legal claims (Schedule 8(6))

This condition is met including where processing is necessary for the purpose of or in connection with any legal proceedings, i.e. where an individual is wanted on warrant by the courts.

Conditions for processing special category and/or criminal conviction data for non-law enforcement purposes, under the UK GDPR.

The processing of personal data during HIOWC's use of LFR to locate missing persons who are at risk of, or pose a risk of, serious risk of harm, or to carry out any future research on the accuracy and efficacy of its use of LFR technology, will be subject to the provisions of the UK GDPR.

a) **Personal data:**

HIOWC's processing of personal data during LFR will satisfy Article 6(1)(e) of the UK GDPR and will be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in HIOWC.

HIOWC's use of LFR for a 'policing purpose' as set out in the SCoP on PIRM demonstrates a public interest in the police, as an official authority, protecting life and property, preventing and detecting crime and safeguarding the vulnerable (including the development of LFR systems, as a tactical tool, to do this).

b) **Special category data:**

HIOWC's processing of special category data during LFR under the UK GDPR will satisfy one of the below lawful bases, dependent on the LFR deployment, curation of the watchlist and whether we are carrying out any research or analysis on the efficacy, accuracy and equitability of our use of LFR as a policing tool.

HIOWC's use of LFR for a 'policing purpose' as set out in SCoP on PIRM demonstrates a substantial public interest in the police, as an official authority, protecting life and property, preventing and detecting crime and safeguarding the vulnerable. HIOWC will always consider whether the use of LFR is necessary and proportionate taking into account consideration of other measures not involving the processing of special category data and whether they could achieve the same outcome.

I. Archiving, research and statistics (Article 9(2)(j))

This condition is met if the processing is necessary for archiving in the public interest, scientific / historical research, and statistical purposes; which is not likely to cause substantial damage or distress, is proportionate and is carried out with safeguards (including security and data minimisation/pseudonymisation) and in the public interest. As a public authority, HIOWC has an ongoing Public Sector Equality Duty (sections 149 – 157, Equalities Act 2010) and future research to support meeting this requirement would be in the public interest.

There is an additional requirement to meet one or more conditions from the DPA 2018 Schedule 1, which are Schedule 1, Part 1 (4) Research

Eg: carrying out research and / or statistical analysis of HIOWC's LFR deployments and LFR technology to develop understanding and improve the accuracy of the LFR technology and the efficacy of LFR as a policing capability; and/or

II. Schedule 1, Part 2 (8) Equality of opportunity or treatment

Eg: carrying out research and/or statistical analysis of HIOWC's LFR deployments and LFR System to identify or keep under review the existence or absence of equality of treatment between groups of people sharing protected characteristics a view to enabling such equality to be promoted or maintained.

III. Substantial public interest (Article 9(2)(g))

This condition is met if the processing is necessary for reasons of substantial public interest, on the basis of law, and is proportionate to the policing purpose / objective pursued. An Appropriate Policy document is in place.

There is an additional requirement to meet one or more conditions from the DPA 2018 Schedule 1, which are:

Schedule 1, Part 2, (6) Statutory and government purposes.

This condition is met if the processing is necessary of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.

Eg: processing of images of persons believed to be missing persons where it is believed it is likely that they could be at risk of coming to serious harm, or pose a risk of causing serious harm; fulfilling the substantial public interest.

Schedule 1, Part 2, (7) Administration of justice

This condition is met if the processing is necessary for the administration of justice e.g. where processing is necessary for the purposes of legal proceedings relating to a missing person.

Schedule 1, Part 2 (8) Equality of opportunity or treatment

Eg: carrying out research and/or statistical analysis of HIOWC's LFR deployments and LFR System to identify or keep under review the existence or absence of equality of treatment between groups of people sharing protected characteristics a view to enabling such equality to be promoted or maintained.

Schedule 1, Part 2 (10) Preventing or detecting unlawful acts

This condition is met if processing is necessary for the purposes of the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as not to prejudice those purposes and is necessary for reasons of substantial public interest.

Schedule 1, Part 2 (12) Regulatory requirements relating to unlawful acts and dishonesty etc.

This condition is met if 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.

Schedule 1, Part 2 (18) Safeguarding of children and individuals at risk

This condition is met if processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, where the individual is aged under 18 or over 18 and at risk, processing is carried out without the data subject's consent because they can't give it or consent can't reasonably be expected to be obtained or obtaining consent would prejudice the protection, and processing is in the substantial public interest.

IV. Criminal conviction and offence data

HIOWC's processing of criminal conviction and offence data during LFR under Article 10 UK GDPR and section 10(5) DPA 2018 will satisfy one or more of the below conditions, dependent on the LFR deployment, curation of the watchlist.

HIOWC's use of LFR for a 'policing purpose' as set out in SCoP on PIRM demonstrates a substantial public interest in the police, as an

official authority, protecting life and property, preventing and detecting crime and safeguarding the vulnerable. HIOWC will always consider whether the use of LFR is necessary and proportionate taking into account consideration of other measures not involving the processing of special category data and whether they could achieve the same outcome.

There is an additional requirement to meet one or more conditions from the DPA 2018 Schedule 1, which are:

Schedule 1, Part 2, (6) Statutory and government purposes.

This condition is met if the processing is necessary of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.

Eg: processing of images of persons believed to be missing persons where it is believed it is likely that they could be at risk of coming to serious harm, or pose a risk of causing serious harm; fulfilling the substantial public interest

Schedule 1, Part 2, (7) Administration of justice

This condition is met if the processing is necessary for the administration of justice e.g. where processing is necessary for the purposes of legal proceedings relating to a missing person.

Schedule 1, Part 2 (8) Equality of opportunity or treatment

Eg: carrying out research and/or statistical analysis of HIOWC's LFR deployments and LFR System to identify or keep under review the existence or absence of equality of treatment between groups of people sharing protected characteristics a view to enabling such equality to be promoted or maintained.

Schedule 1, Part 2 (10) Preventing or detecting unlawful acts

This condition is met if processing is necessary for the purposes of the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as not to prejudice those purposes and is necessary for reasons of substantial public interest.

Schedule 1, Part 2 (12) Regulatory requirements relating to unlawful acts and dishonesty etc

This condition is met if 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.

Schedule 1, Part 2 (18) Safeguarding of children and individuals at risk

This condition is met if processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, where the individual is aged under 18 or over 18 and at risk, processing is carried out without the data subject's consent because they can't give it or consent can't reasonably be expected to be obtained or obtaining consent would prejudice the protection, and processing is in the substantial public interest.

Schedule 1, Part 3 (30) Protecting individual's vital interests

This condition is met if processing is necessary to protect the vital interest of an individual and the data subject is physically or legally incapable of giving consent.

Schedule 1, Part 3 (30) Personal data in the public domain

This condition is met if processing relates to personal data which is manifestly made public, in the sense of being realistically accessible to the public or part of the public, by the data subject.

Schedule 1, Part 3 (33) Legal claims

This condition is met if processing is necessary for the purpose of or in connection with any legal proceedings.

Schedule 1, Part 3 (36) Extension of substantial public interest conditions

This condition is met if processing would meet a condition in Schedule 1 Part 2 but for the express requirement that processing be necessary for reasons of substantial public interest.

Principle (2): purpose limitation

HIOWC is authorised by law to process personal data for the 'policing purposes' set out in the SCoP on PIRM and the Law Enforcement purpose (DPA 2018, Part 3). We may process personal data collected for any one of these 'policing purposes' and LE purposes (whether by us or another controller), for any of the other 'policing purposes' and LE purposes, providing the processing is necessary and proportionate to that purpose. This means that in particular we consider: what we seek to achieve, whether there are alternative measures which would not involve sensitive processing but which would achieve substantially the same outcomes, and the same or lesser impact on individuals and the community.

Watchlist – purpose limitation:

HIOWC's LE purposes for using LFR are primarily the prevention, investigation, detection and prosecution of criminal offences but also the safeguarding against and the prevention of threats to public security. On each occasion that LFR is used, the relevant specific and legitimate LE purpose will be explicitly recorded in the LFR Deployment Application and LFR Deployment Authorisation.

HIOWC will compile the LFR watchlist for each deployment from images previously collected and stored on our IT systems. In nearly all circumstances these will be images collected when a person has been arrested and detained in police custody and which are lawfully held. Their subsequent use in the watchlist is not incompatible with the purpose for which they were originally collected and is underpinned by section 64A of the Police and Criminal Evidence Act 1984. We will not process personal data for purposes that are incompatible with the original purpose for which it was collected.

HIOWC's use of LFR to locate missing persons considered at increased risk of harm, will be subject to the provisions of the UK GDPR. Where HIOWC do not possess an image of the missing person the LFR Authorising Officer will authorise the use of an image of suitable quality, which may be provided by the missing person's family or sourced from open source social media. If the police already hold an arrest / custody photo of the missing person, its inclusion in the watchlist must be 'authorised by law', as required by section 36(4) of the DPA 2018. HIOWC's objective of trying to locate a missing person at risk of serious harm satisfies a 'policing purpose' set out in the SCoP on PIRM, and therefore satisfies the requirement of being 'authorised by law'.

Live LFR CCTV Feed – purpose limitation:

Via the LFR CCTV feed, HIOWC will be collecting images of persons passing through the recognition zone. These images will be collected for a 'policing purpose' relevant to the specific objective of each LFR deployment which will be recorded in the LFR Deployment Application and LFR Deployment Authorisation.

The data uploaded to and collected by LFR systems will only be used for the purposes of:

- Delivering the LFR deployment;
- Responding to citizens' requests to exercise their data subject rights under the DPA 2018 and UK GDPR, or complaints and claims;
- In relation to any subsequent investigations and / or prosecutions if a person on a watchlist is arrested as a direct result of facial matching. This may involve sharing with other LE agencies such as the Crown Prosecution Service, where it is necessary and proportionate to do so.

Principle (3): data minimisation

HIOWC's processing of personal data for LFR will be adequate, relevant and not excessive and will be necessary for the policing purpose / objective it was deployed for.

The below data minimisation measures are set out in the HIOWC LFR Policy and Standard Operating Procedure:

- HIOWC's intelligence led deployments of LFR will ensure that inclusion of images on the watchlist will be limited to only those that are lawfully held and that are relevant to the specific objective of each deployment.
- In addition, the images used in the watchlist will be of adequate quality for comparison e.g. an image of a face with a minimum of fifty pixels between the eyes of the subject. For LFR, this is sufficient to enable a facial biometric data to template to be extracted to compare against a database.
- The collection of images of citizens passing though the LFR recognition zone will be limited to only that which is necessary by ensuring LFR is only deployed where there is an intelligence case supporting its use and efficacy. We will have considered and ruled out using other policing tactics that do not involve collateral collection of data due to them not being effective or have been considered and believed that they would not be effective.
- The positioning of the recognition zone and live feed LFR cameras will avoid particularly sensitive locations where there is an enhanced expectation of privacy or sensitivity unless in rare circumstances where it is absolutely necessary to do so for the specific objective of the deployment.
- The storage of data collected and used for LFR will be minimised by securely disposing of it as soon as it is no longer required for an LFR related purpose, detailed in section 5 and Appendix 1, below.

Principle (4): accuracy

Watchlist:

The source of the vast majority of images that will populate the watchlist is HIOWC's Niche Record Management System (RMS) that holds the necessary custody arrest images. The extraction of these images needed for each individual watchlist will be executed by specific inclusion criteria within an automated script. The script will be developed and tested prior to live deployment and enable the categorisation of images relative the specific policing purpose driving their inclusion on the watchlist. Metadata of the extracted watchlist images will be reviewed pre-deployment, via a CSV file, to ensure that any persons falling within specified categories, such as children aged under 13 or between 13 and 18, can be identified and highlighted for the benefit of the Authorising Officer and in the briefing to LFR staff.

The watchlist will be complied no longer than 24 hours prior to each LFR deployment. The watchlist will then be deleted from the LFR system no later than 24 hours after the end of each deployment.

Quality of custody images:

HIOWC will only use images where all reasonable steps have been taken to ensure that the image:

- is of a person intended for inclusion on a given watchlist;
- is lawfully held and therefore relatively recent; and
- is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the watchlist. Regard will be paid to the prospect of the LFR application generating an Alert/False Alert should an older image be proposed for inclusion where the person's facial features may have changed or

aged significantly since the image was taken. Any non-compliant images proposed to be included in the watchlist will be highlighted in the LFR Application.

Accuracy of the algorithm and LFR system:

The LFR algorithm that HIOWC uses in its LFR system has undergone evaluation by the National Institute of Standards & Technology in 2018 where it was held in high regard. In 2023 the National Physical Laboratory conducted an evaluation of the algorithm (commissioned by South Wales Police (SWP) and the Metropolitan Police Service: frt-equitability-study_mar2023.pdf (science.police.uk)).

As part of HIOWC's ongoing activity to meet its Public Sector Equality Duty we have undertaken due diligence to the expected algorithm performance, having regard to publicly available research, the detail of which can be found in the HIOWC Human Rights Impact Assessment, Equality Impact Assessment and Data Protection Impact Assessment (Live Facial Recognition Technology | Hampshire and Isle of Wight Constabulary). We have also considered the outcomes of other force deployments; SWP regularly undertake large-scale Facial Recognition system deployments. HIOWC will also provide for an ongoing evaluation of the algorithm accuracy, efficacy and equitability via a post-deployment review process on a per deployment basis.

The LFR system has an algorithm threshold setting which affects the accuracy of its facial matching. Fixing this value too low or too high can, respectively, create risks of a high False Alert Rate (incorrect match alert identified by the software) or a high False Negative rate (software has failed provide an alert when someone on the watchlist has passed by the LFR cameras). As set out in the HIOWC LFR Policy, HIOWC will use a threshold setting of 0.64, which is the configuration at which the National Physical Laboratory's scientific testing found equitability of the FPIR and TPIR was achieved across all demographics. This is a higher threshold setting than the minimum threshold setting recommended by NPL. SWP's experience of using of this threshold setting is that its LFR system has reliably resulted in no false alerts / matches.

When citizens pass through the LFR recognition zone not every person that is captured via the live CCTV camera feed will be enrolled into the LFR system. The captured image of a citizen's face has to be of sufficient 'quality' to be enrolled into the LFR system. The level of enrolment rate will be dependent on many environmental factors, the more significant of these include: crowd density, individual movements, face angle and lighting.

When the LFR system provides an alert on a potential match the LFR Operator will always make a decision as to whether they believe it is the same person. No action will be taken against an individual without human consideration of a valid match. On making that decision the LFR operator will be provided with:

- The two images for comparison both side by side and the ability to overlay them.
- A numerical matching score.
- An indication of the quality of the image.
- An indication of how long ago the watchlist photo was taken.
- The reason why the person was on the watchlist.

Where the LFR operator believes the two images to be the same person they will notify the Engagement Officer who will then independently decide whether to engage the individual, ask for identification and take any subsequent appropriate policing action.

Training:

The only officers operating the LFR system are trained LFR Operators. A small number of Engagement Officers will make the final decision on potential matches and whether to make any engagement with the individual. The LFR Silver Commander will provide an appropriate LFR briefing to Engagement Officers however the decision making and execution around whether to engage an individual is no different in an LFR context than it is for other operational policing contexts.

Right to rectification:

HIOWC has a specialist team that will consider any submitted citizens' data subjects rights requests, as provided for under the DPA 2018 and UK GDPR. Requests asking for any inaccurate data to be rectified or erased will be actioned within the statutory time period of one month. Where we become aware that personal data contained within a watchlist is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision and take appropriate steps to inform the data subject. Where we erase or rectify personal data we will inform any recipients with whom we have shared that data.

Law enforcement specific accuracy requirements (DPA 2018, Part 3):

Section 38(2) of the DPA 2018 requires that for any of the LE purposes that personal data based on fact must be distinguished from personal data based on personal assessments, so far as possible. The LFR system achieves this by effectively indicating its confidence in the potential match through the match score and the LFR system operators and Engagement Officers contextually understand that any potential match alerts produced by the LFR system are not fact but are a technical assessment that helps supplement the officers' human assessment.

Section 38(3) of the DPA 2018 requires that for any of the LE purposes a clear distinction must be made, where relevant and as far as possible, between personal data relating to different categories of data subject. The images of persons included on the watch list will be categorised and labelled as per the policing objective of their inclusion (eg: wanted on court warrant or suspect of criminal offence will contextually be categorised as a suspect as opposed to a missing person at increased risk of harm).

Principle (5): storage limitation

The retention and disposal of personal and sensitive special category data processed by the LFR system and the supporting processes is detailed in the table shown in Appendix 1.

We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. An example would be if another individual's image was captured that was not subject to an enquiry.

The age of images (sourced from HIOWC's RMS system) selected for copying into the watchlist are in line with the College of Policing's Authorised Professional Practice on Information Management (Review, retention, disposal and custody images) which supports the Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4).

Principle (6): integrity and confidentiality (security)

Data Protection Polices are applied from inception of initiatives to ensure legislative compliance with our data protection obligations and to determine appropriate levels of technical and organisational safeguards and controls when processing personal data and sensitive data. All of our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

Our electronic systems and physical storage have appropriate access controls applied including for example, multi-factor authentication to access mobile devices (in the form of multiple sign in/access codes/facial recognition etc), password protection, encryption and locking mechanisms. Information Asset Owners are responsible for ensuring that all information management processes are applied to information and there is a continuous cycle of review and information risk identification and management. LFR has also been subject to a robust DPIA.

The RMS system, from which custody photos are copied for the watchlist, is hosted within our accredited secure computer network in accordance with national and local security policies. Copies of deployment records and strategic LFR documentation (such as policies, procedures data protection governance documentation are also stored within this secure network.

The watchlist photos will be selected via a fully tested script and downloaded onto a HIOWC provided encrypted USB, using a specifically enabled computer asset. Events that take place on operational systems are recorded on an audit log which enables identification of the action executed, when it was carried out and by whom.

The images will be uploaded to the LFR system by a member of the LFR Team via an encrypted USB. The LFR system is an isolated closed system and does not sit on the HIOWC IT network. On each deployment day, the encrypted USB will remain the responsibility of a named individual of the LFR Team to ensure it remains secure and is available for deletion / wiping of images at the end of each deployment day. The LFR Silver Commander is accountable for ensuring this occurs. The watchlist is deleted off the LFR system within 24 hours of the conclusion of each deployment.

The LFR system has been assessed by the HIOWC Information assurance Team.

LFR operators are the only persons that will be operating the LFR system and are vetted police officers who are trained and experienced in operating the LFR system securely.

LFR Engagement Officers will not operate the LFR system but will make the ultimate decision on whether engage an individual that is believed to be a match by the LFR operator. A specific LFR briefing is provided to the Engagement Officers and Silver Commander. This training is also supplemented with bespoke Standard Operating Procedures. All HIOWC staff must also undertake mandatory basic data protection training and refresher training for managing information.

ACCOUNTABILITY PRINCIPLE

HIOWC have put in place appropriate technical and organisational measures to meet the requirements of accountability and to demonstrate compliance with wider requirements of Part 3 of the DPA 2018, the UKGDPR and in particular the principles. These include:

- The appointment of a Data Protection Officer who is responsible for data protection compliance for LFR.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining a record of processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with any data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out Data Protection Impact Assessments for our high-risk processing.
- We have an Information Management Policy.

We regularly review our accountability measures and update or amend them when required.

If any future HIOWC statistical research to analyse and develop the accuracy and efficacy our use of LFR systems, is carried out on our behalf by a third party, this relationship will be governed by a data processing contract (if necessary) and designed with advice from HIOWC's Data Protection Officer.

APPROPRIATE POLICY DOCUMENT REVIEW DATE

This policy will be retained for 6 years after the cessation of HIOWC's use of LFR. It will be reviewed annually or revised more frequently if necessary.

Account is taken of all regulatory and policing information and guidance, relevant case law and changes to legislation.

A copy of this policy will be published on the HIOWC website and a copy is available to the Information Commissioner, on request, free of charge in accordance with s42(3)(c) DPA.

Policy document Sign-Off

Person completing the APD	Name (in capitals)	**Sharon Warwick – Senior Information Governance Manager**
	Date:	Reviewed & updated: 05/12/2025

Data Protection Officer	Name:	**Jason Saxon – Director of Data & Information**
	Date:	09/12/2025
Approval Signature (Approval will be required by either the Data Protection Officer	Signed:	*Jason Saxon*

Appendix 1 – Table of Retention Periods for LFR Data

Personal Data	Retention Period	Rationale	Deletion Accountability
Source image on HIOWC RMS system from which a copy is taken from for the watchlist	N/A – out of scope of LFR processing	The retention of source images are used for broader policing purposes outside of LFR. Retention framework provided for by: Review, retention & disposal | College of Policing (APP)	N/A out of scope of LFR
Watchlist images and biometric templates on LFR system	Deleted at the end of each days deployment and at the latest within 24 hours of end of deployment.	Technical functionality. Updated for each day's deployment to remain accurate and up to date for operational use and for security purposes.	LFR System Operator
Watchlist: CSV file of meta data of persons on watchlist	Deleted at the end of each days deployment and at the latest within 24 hours of end of deployment.	Allows time to record any de-personalised watchlist make-up data for longer term analysis.	LFR System Operator
Watchlist: copy of watchlist images on USB to import onto LFR system	Data securely removed within 24 hours of the conclusion of each days' deployment.	A new watchlist is needed and created no longer than 24 hours before each day's deployment to ensure it remains up to date.	LFR Silver Commander for each deployment
Recognition zone: CCTV footage from Recognition zone LFR cameras	Removed from LFR system then retained for: 1) 31 days by default. Retained for longer by exception if: 2) Retained in relation to investigate a complaint about officer conduct. 3) Retained as evidence for a criminal offence investigation / prosecution	1) National non-evidential CCTV retention period. 2) 6 years after complaint / investigation closed (National Police Chiefs Council Retention Policy). 3) As per Criminal Procedure & Investigations Act (CPIA)1996 and APP	1) Strategic LFR Lead
Recognition zone: image and biometric template	Deleted from LFR system as per following scenarios: 1) No match / alert = instant deletion.	1) Automatic LFR system functionality.	1) Automated LFR functionality

	2) True or false alert / match = deleted at end of each days' deployment or 24 hours	2) Technical functionality.	2) LFR System Operator
Personal Data	**Retention Period**	**Rationale**	**Deletion Accountability**
Deployment Logs for each specific deployment - containing personal data	1) Deployment Record: as soon as practical but within 31 days 2) Match Report as soon as practical but within 31 days.	1) To carry out a retrospective review of the management of the deployment as a whole 2) For secondary, retrospective review of any matches flagged by the LFR system and subsequent engagements.	1) & 2) LFR Silver Commander for each deployment
Records for each specific deployment (not containing personal data).	Retained for 6 years after specific deployment Following types of records: • Deployment Log; • Deployment authorisations; • LFR numerical results for publication; • LFR Cancellation Reports; • LFR Register of Deployment; • Community Impact Assessments.	Retained for: • Legal reasons: dealing with complaints / challenge. • Development / analysis of the use of LFR systems.	Strategic LFR Lead
Over-arching LFR Policies, Procedures etc. (not containing personal data).	Retained until 6 years after HIOW has ceased use of LFR systems. Following types of records: policy, standard operating procedure, legal mandate, impact assessments, privacy notice, appropriate policy document, training content.	Retained for: • Legal reasons: dealing with complaints / challenge. • Development / analysis of the use of LFR systems.	Strategic LFR Lead
Any future accuracy / efficacy research (probe and watchlist images used for comparison)	To be determined at the time any future research is scoped. Will be retained no longer than necessary.	UK GDPR article 5(1)(e) recognises and permits research data to be kept for longer periods provided safeguards are in place (s.19 DPA 18 and a.89 UK GDPR).	Strategic LFR Lead