



Thames Valley Police

Appropriate Policy Document for the Processing of Special Category and Criminal Data for overt Use of Live Facial Recognition

This is the 'appropriate policy document' that sets out how Thames Valley Police (TVP) will protect special category and criminal conviction personal data in compliance with Part 3 of the Data Protection Act 2018 (DPA 2018) and UK GDPR.

'Special category' data or 'sensitive' data is personal data that reveals:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data or biometric data for the purposes of uniquely identifying and individual,
- health,
- sex life and sexual orientation.

Part 3 of the DPA 2018, which stipulates the provisions for processing personal data for law enforcement purposes, names the above data 'sensitive data'. The UK GDPR, which stipulates the provisions for processing personal data for general purposes, names the same data as 'special category data'. This document will refer to the above data as 'sensitive data' for ease of use.

The UK GDPR refers to 'criminal data' as personal data relating to:

- criminal convictions and offences, and
- related security measures.

It does not cover personal data about victims and witnesses related to criminal convictions / offences.

1. Introduction

Sections 35(3), 35(5)(c) and 42 in Part 3 of the DPA 2018 set out the requirement for an appropriate policy document to be in place when conducting sensitive processing for Law Enforcement purposes.

Schedule 1, Part 4 of the DPA 2018 sets out the requirement for an appropriate policy document to be in place when processing special category data under the UK GDPR.

The purpose of this document is to explain:

- TVP's procedures which are in place to secure compliance with the six data protection principles set out in:
 - Part 3, section 34 of the DPA 2018 and in reliance of one of the conditions set out in Schedule 8; and
 - Article 5 of the UK GDPR and in reliance of one of the conditions set out in article 9 of the UK GDPR and schedule 1 of the DPA 2018.
- TVP policies about the retention and erasure of such personal data processed in reliance on a condition specified in Schedule 8 to the DPA 2018 and article 9 and schedule 1 of the UK GDPR.

This 'appropriate policy document' reflects the requirements to have safeguards in place for sensitive processing carried out for a law enforcement purpose as set out in section 42 and Schedule 1 (Part 4) of the DPA 2018.

2. Description of personal data processed during live facial recognition use:

The TVP LFR deployments will be delivered using specialist equipment operated by the Thames Valley Police and Hampshire & Isle of Wight Constabulary 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. The Chief Constable of TVP will be the data controller for deployments conducted by TVP, for the purpose of TVP's policing objectives in the TVP geographical area.

Live facial recognition (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. The sensitive 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 TVP custody image dataset but may also include other lawfully held images. These custody images have been previously collected by TVP 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.

TVP will use LFR technology to locate persons listed below, in support of its policing objectives:

- a) Wanted by way of an outstanding warrant for their arrest issued by a court or are sought for recall to prison.
- b) About whom there are reasonable grounds for suspecting that they have committed a criminal offence.
- c) Who are subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment.
- d) Who are currently subject to legally enforceable restrictions or conditions, in order to monitor compliance with those restrictions or conditions, where compliance can be monitored through the individual's presence, conduct or both, within the deployment location. This includes MAPPA subjects (including registered sex offenders) and persons subject to police or court-imposed conditions, such as bail conditions or court orders, where the restrictions or conditions relate to relevant offences.
- e) About whom there is credible intelligence, a known history of relevant and recent offending, or both, that gives rise to reasonable grounds for suspecting that they are likely to commit a serious or hotspot crime, pose a risk to public safety, or cause other harm, including self-harm.
- f) Who are designated as a Missing Person.
- g) About whom there is credible intelligence that gives rise to reasonable grounds for suspecting that they are at real risk of serious harm.
- h) About whom there is credible intelligence that gives rise to reasonable grounds for suspecting that they are likely to be a victim of, or witness to, a serious crime.

In respect of all persons sought, both the seriousness of the suspected offence or other harm, and its prevalence and local impact will be considered.

Statistical analysis may be carried out to analyse and develop the accuracy, efficacy and equitability of TVP's use of LFR systems. Any processing of images and LFR data for this reason would not involve the need to identify or locate persons. Such analysis would be subject to the additional safeguards such as de-personalisation and would not result in any decisions with respect to a particular individual.

3. Compliance with data protection principles

a) 'Lawfulness, fairness and transparency'

Lawful:

TVP's use of LFR must not be unlawful in a broad sense as well as satisfying a specific lawful basis for the use of personal data, sensitive data and criminal data.

TVP has a number of long-established policing responsibilities and powers derived from common law which have been recognised by the courts. These responsibilities are described as 'policing purposes' in the Statutory Code of Practice on Police Information and Records Management as:

- 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.

TVP's use of the police custody photos of the persons of interest placed on the LFR watchlist is lawful under section 64A of the Police and Criminal Evidence Act 1984, for the purposes of prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

As a public authority, TVP's use of LFR must be in compliance with the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights: the right to respect for private and family life, home and correspondence:

*"There shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, **public safety** or the economic well-being of the country, for the **prevention of disorder or crime**, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

TVP ensures that LFR related article 8 interference is qualified and permissible by:

- TVP's LFR use is underpinned by common law providing a legal basis which is made accessible and foreseeable to the public by TVP publishing a comprehensive set of its LFR documents on its website: [Live Facial Recognition Technology | Thames Valley Police](#)
- TVP ensures its use of LFR satisfies the legitimate aim of public safety and the prevention of disorder and crime and pressing social need by the careful intelligence led curation and Authorising Officer authorisation of the LFR watchlist to meet the policing objectives of locating persons for reasons listed in section 2 (listed a – h).
- TVP will ensure its use of LFR is necessary by only deploying 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.
- TVP will ensure its use of LFR considers the intrusion into the public's broader human rights and right to privacy to ensure that it is proportionate to its legitimate aim of public safety and the prevention of disorder and crime. When deciding: watchlist curation, location of the LFR recognition zone, time and date of deployment and LFR system settings; particular attention will be given to reducing privacy intrusion.

Lawful Bases:

TVP's processing of personal data for LFR will mostly fall under DPA 2018 Part 3 for a law enforcement purpose.

Data Protection Act 2018, Part 3 processing:

Personal data:

The processing of personal data during the use of LFR will be necessary for the 'Law Enforcement' 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.

TVP's processing of personal data for LFR must also be 'authorised by law' which is met by the 'policing purpose' set out in the Statutory Code of Practice on Police Information and Records Management.

TVP will not rely on individual's the consent to process their personal data for LFR purposes.

Sensitive data:

TVP will not rely on individual's the consent to process their sensitive data for LFR purposes and therefore TVP relies on the following conditions from Schedule 8 of the DPA18 and has an appropriate policy document in place:

- **Statutory etc. purposes (Schedule 8(1)):** 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.
- **Administration of justice (Schedule 8(2)):** processing is necessary for the administration of justice.
- **Protecting individual's vital interests (Schedule 8(3)):** processing is necessary to protect the vital interests of the data subject or another individual.
- **Safeguarding of children and of individuals at risk (Schedule 8(4)):** processing is necessary to protect individuals, under 18yo or over 18yo and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.
- **Personal data already in the public domain (Schedule 8(5)):** processing relates to personal data which has been manifestly made public by the data subject.
- **Legal claims (Schedule 8(6)):** processing is necessary for in connection with legal proceedings, obtaining legal advice, or establishing / exercising / defending legal rights.

UK GDPR processing:

The processing of personal data to locate missing persons and carrying out any future research into the accuracy and efficacy of TVP's use of LFR, which will fall under the UK GDPR.

Personal data:

TVP's processing of personal data during the use of LFR will satisfy:

- **Article 6(1)(c):** processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Article 6(1)(d):** processing is necessary to protect the vital interests of the data subject or another natural person.
- **Article 6(1)(e):** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in TVP.

Special category data:

TVP will not rely on individual's consent to process their special category data for LFR purposes and therefore TVP relies on the following conditions from article 9(2) of the UK GDPR and Schedule 1 of the DPA 2018 and has an appropriate policy document in place:

- **Article 9(2)(c):** processing 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)(e):** processing relates to personal data which are manifestly made public by the data subject;
- **Article 9(2)(g):** processing necessary for reasons of substantial public interest provided for in domestic law. The substantial public interest conditions require a condition from Part 2 of Schedule 1 of the DPA 2018 to be satisfied, as follows:
 - **Schedule 1, Part 2(6) Statutory and government purposes:** 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 1, Part 2(8) Equality of Opportunity or Treatment:** processing is necessary for the purposes 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.
 - **Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk:** processing is necessary to protect individuals, under 18yo or over 18yo, and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

Criminal data:

TVP will process criminal offence data during LFR deployments and under Article 10 of the UK GDPR and section 10(5) of DPA 2018 the processing must satisfy a condition from Parts 1-3 of Schedule 1 of the DPA 2018. TVP meets the following conditions:

- **Schedule 1, Part 2(6) Statutory and government purposes:** 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 1, Part 2(8) Equality of Opportunity or Treatment:** processing is necessary for the purposes 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.
- **Schedule 1, Part 2(18) Safeguarding of children and of individuals at risk:** processing is necessary to protect individuals, under 18yo or over 18yo, and at risk from neglect or physical, mental or emotional harm; or protecting the physical, mental or emotional wellbeing of an individual.

Fairness & Transparency:

TVP will only use personal data for LFR in ways that the public would reasonably expect and not use it in ways that have unjustified adverse effects on them. Members of the public would expect TVP to use its available information and tactical capabilities to locate persons of interest: who are wanted (on warrant, recall to prison, suspected of / likely to commit an offence); to enforce court or police-imposed orders / conditions; who pose a risk of harm or are at risk of harm; missing persons; or a victim / witness to a serious crime.

TVP will publicise its LFR deployment 7 days in advance of a deployment on its social media channels and on the LFR page on the TVP internet site. During a LFR deployment, TVP will place visible signs ahead of entry points into the recognition zones so that members of the public will be aware of its location.

TVP will publish, on its LFR website page, the following documents:

- Legal Mandate
- LFR policy and procedures
- Impact assessments,
- Data Protection Impact Assessment,
- LFR specific Privacy Notice,
- Notice of future deployments
- Retrospective analysis of retrospective LFR deployments.

Unjustified adverse effects of any inaccurate facial matching are mitigated by selecting a LFR system accuracy threshold setting of 0.64, where inaccurate matches have been shown to be highly unlikely. A TVP officer will review the proposed match and make a final decision on whether they believe it to be a match before deciding whether to engage the individual.

b) 'Purpose limitation'

TVP is authorised by law to process personal data for the 'policing purposes' set out in the Statutory Code of Practice on Police Information and Records Management and the law enforcement purpose (DPA 2018, Part 3). We may process personal data collected for any one of these 'policing purposes' (whether by us or another controller), and law enforcement purposes, for any of the other 'policing purposes' and law enforcement 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.

TVP will not process personal data for purposes incompatible with the original purpose for which it was collected. We will not process data collected for a law enforcement purpose (under DPA2018 Part 3) for a purpose that is not a law enforcement purpose (under UK GDPR) unless the processing is 'authorised by law' as required by section 36(4) of the DPA 2018.

For each individual LFR Deployment the specific relevant law enforcement and / or policing purpose will be explicitly recorded in the LFR Deployment Application and authorised by a specific 'Authorising Officer in the LFR Deployment Authorisation.

In nearly all circumstances the photos on TVP compiled LFR watchlist will be from images of persons arrested and detained in police custody and therefore already in TVPs possession. Further use of police custody images for LFR is not incompatible with the original purpose of collection and is supported by section 64A of the Police and Criminal Evidence Act 1984.

Where a police custody image (collected for a law enforcement purpose) is used on an LFR watchlist to locate a missing person (a non-law enforcement purpose), the processing will be subject to the provisions of the UK GDPR and must satisfy section 36(4) of the DPA 2018 and be 'authorised by law'. Its use is 'authorised by law' by satisfying the 'policing purpose': protecting life and property, as set out in the Statutory Code of Practice on Police Information and Records Management.

Where TVP do not possess an image of a 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

During a TVP LFR deployment the LFR CCTV feed 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 CCTV feed 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 law enforcement agencies such as the Crown Prosecution Service, where it is necessary and proportionate to do so.

Statistical analysis may be carried out to analyse and develop the accuracy, efficacy and equitability of TVP's use of LFR systems. Any processing of images and LFR data for this reason would not involve the need to identify or locate persons. Such analysis would be subject to the additional safeguards such as de-personalisation and would not result in any decisions with respect to a particular individual.

c) 'Data minimisation'

TVP only collects sensitive data that is necessary and proportionate to carry out the law enforcement and policing purposes. It is processed in the context of carrying out processes which enable us to meet our stated law enforcement purposes for processing.

TVP'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 designed into the TVP's use of LFR systems and deployments:

- TVP'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 objectives of each deployment.

- Images used in the watchlist will be of adequate quality for comparison and sufficient to enable a facial biometric data template to be extracted to compare against a database.
- The collection of images of the public passing through 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 e) and Appendix 1, below.

d) 'Accuracy'

Under the Equalities Act 2010, TVP as a public authority has an ongoing Public Sector Equality Duty to eliminate unlawful discrimination based on any of the protected characteristics; which will extend to its use of LFR.

TVP has undertaken due diligence to the expected performance of the TVP LFR system. This includes the review and consideration of publicly available information including an evaluation in 2023 by the National Physical Laboratory who evaluated the LFR algorithm (commissioned by South Wales Police and the Metropolitan Police Service who use the same LFR system: [frt-equitability-study_mar2023.pdf \(science.police.uk\)](https://www.science.police.uk/sites/default/files/2023-03/frt-equitability-study_mar2023.pdf)).

The TVP LFR system has an algorithm threshold setting which affects the accuracy of its facial matching. The National Physical Laboratory's scientific testing found that at a setting of 0.64 there was equitability of facial matching accuracy across all demographics. In TVP's consideration of the threshold setting it will adopt, it has reviewed the LFR deployments made by South Wales Police where (at the time of writing this document) no inaccurate matches were experienced at a threshold setting of 0.64. TVP will deploy LFR with an accuracy setting of 0.64 and carry out its own equitability evaluation after each deployment.

TVP has carried out and documented an Equality Impact Assessment of its LFR system use, including the environmental factors affecting LFR camera set up, which will be published on the TVP LFR website page: [Live Facial Recognition Technology | Thames Valley Police](#)

Broadly the inclusion of poor quality photos in the watchlist can have an impact on the accuracy of facial matching. TVP will predominantly use custody images for watchlist compilation and are required to ensure that the custody images are of sufficient quality to be used effectively in their systems. The LFR system will reject the upload of a watchlist image onto the LFR system if the image fails to meet the minimum image quality required by the LFR system.

The TVP LFR system operators are trained to take into account the environmental factors of the recognition zone and expected density of the public moving through it, when setting up the LFR cameras for each deployment.

When the LFR system alerts that a potential match has been found the TVP LFR operator is provided with several pieces of information to help them decide whether they believe it is an accurate match. These are: a matching score, image quality indication, the ability to overlay the watchlist and live feed image over each other, and an indication of how long ago the image was taken. If the LFR system operator determines the two images are a match they will notify the TVP Engagement Officer who will then independently consider whether they believe them to be a match and if so whether to engage that individual, confirming their identification when they do so.

Under the DPA 2018 (Part 3) and UK GDPR, all individuals have a right to ask an organisation processing their personal data to amend or append any inaccurate data held about them. TVP has a specialist team that will consider any submitted requests within the statutory time period of one month.

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

- Section 38(2) of the DPA 2018 requires that for any of the law enforcement 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 law enforcement 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.

e) 'Storage limitation'

All personal, sensitive and criminal data processed by TVP for LFR is retained for the periods set out in the retention schedule set out in Appendix 1.

For members of the public passing through the LFR recognition zone, 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 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.

The CCTV live feed capture of members of the public passing through the recognition zone is deleted after 31 days unless by exception it is required to be kept retained for longer:

- Retained in relation to investigate a complaint about officer conduct.
- Retained as evidence for a criminal offence investigation / prosecution

The retention and deletion custody images stored on TVP's crime recording system, from which the watchlist images are sourced, will be managed outside of the LFR processing; in accordance with the retention guidance set out in the Statutory Code of Practice on Police Information and Records Management and associated [College of Policing's Authorised Professional Practice on Information Management](#)

The images on the LFR watchlist will be deleted within 24 hours of the completion of the LFR deployment.

f) 'Integrity and confidentiality'

TVP comply with the relevant parts of the legislation relating to security, and seek to comply with the [College of Policing - Information Assurance Authorised Practice](#) and relevant parts of the ISO27001 Information Security Standard.

TVP standard operating procedures and policies make clear what use may be made of any sensitive data contained within them. Our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. The security of the LFR system has been assessed by the TVP ICT department.

All force staff and officers are subject to pre-employment police vetting checks and periodical vetting checks once in post. All force staff have to undergo mandatory data protection and security training.

Any security incidents involving sensitive data are fully and corporately recorded, investigated and assessed for whether they should be reported to the Information Commissioners Office.

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.

The LFR system is an isolated closed system and does not sit on the TVP IT network. It is operated only by trained TVP LFR operators. On each deployment day, the encrypted USB will transfer the watch list images to the LFR system and will remain the responsibility of a named TVP LFR Team individual to ensure it remains secure and is available for deletion / wiping of images at the end of each deployment day. The watchlist is deleted off the LFR system within 24 hours of the conclusion of each deployment.

During active LFR deployments, a uniformed constable remains with the vehicle to maintain physical security. If the vehicle is left unattended, the watchlist is erased from the database.

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.

Copies of deployment records and strategic LFR documentation are stored within the TVP secure network.

g) 'Accountability'

TVP demonstrates how its use of LFR meets the requirements of the DPA 2018 (Part 3 in particular) and UK GDPR with the following measures which will be reviewed and updated when required:

- Conducting and publishing a Data Protection Impact Assessment, reviewed by the Data Protection Officer.
- Publishing a LFR specific privacy notice and appropriate policy document.
- Publishing a retention schedule for the different types of personal data processed during LFR.
- Designing LFR processes to take into account data protection requirements.
- Carrying out a security assessment of the LFR system and implementing appropriate security measures.
- Having an Information Management Policy and LFR Policy.
- Having written contracts with any data processors.
- Recording LFR activity in TVP's Record of Processing Activities.

If any future TVP 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).

4. Further Information

For further information about our compliance with data protection law or if you wish to contact

Thames Valley Police Data Protection Officer:

Thames Valley Police
Public Access Office
Oxford Road
Kidlington
OX5 2NX

Email: publicaccess@thamesvalley.police.uk

5. Requirement to keep records

Where sensitive processing is carried out by TVP (as the data controller), the following information is recorded in its Record of Processing Activities:

- whether the sensitive processing is carried out in reliance on the consent of the data subject, or if not, which condition in Schedule 8 is relied on;
- how the processing satisfies section 35 (lawfulness of processing); and
- whether the sensitive data is retained and erased in accordance with the policies described above in section 3 of this document, and, if it is not, the reasons for not following those policies.

This LFR Appropriate Policy Document will be retained for 6 months beyond the strategic cessation of LFR as a policing tactic. To ensure the Appropriate Processing Document remains up to date it will be reviewed regularly and any relevant information from the Record of Processing Activities will be included where it is appropriate to do so.

Appendix 1 – Table of Retention Periods for LFR Data

Personal Data	Retention Period	Rationale	Deletion Accountability
Source image on TVP's 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.	1) National non-evidential CCTV retention period. 2) 6 years after complaint / investigation closed (National Police Chiefs Council Retention Policy).	1) Strategic LFR Lead

	3) Retained as evidence for a criminal offence investigation / prosecution	3) As per Criminal Procedure & Investigations Act (CPIA)1996 and APP	
Personal Data	Retention Period	Rationale	Deletion Accountability
Recognition zone: image and biometric template	Deleted from LFR system as per following scenarios: 1) No match / alert = instant deletion. 2) True or false alert / match = deleted at end of each days' deployment or 24 hours	1) Automatic LFR system functionality. 2) Technical functionality.	1) Automated LFR functionality 2) LFR System Operator
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,	Retained for: • Legal reasons: dealing with complaints / challenge. • Development / analysis of the use of LFR systems.	Strategic LFR Lead

	privacy notice, appropriate policy document, training content.		
Personal Data	Retention Period	Rationale	Deletion Accountability
Any future accuracy / efficacy analysis or evaluation	To be determined at the time any future research is scoped. Will be retained no longer than necessary		Strategic LFR Lead

Document Review Information			
Version History	Version Date	Requestor of Change	Summary of Change(s)
0.1	01/12/2025	N/A	First Draft
1.0	12/12/2025	Senior Information Governance Manager & Head of Intelligence	Final changes for publication before implementation
2.0	29/07/2026	Senior Information Governance Manager & Head of Intelligence	Updated use cases for inclusion of persons on watch list