Appropriate Policy Document: Live Facial Recognition

Sensitive Processing for General Processing

Greater Manchester Police (GMP) is a Police Force established under the Police Act 1996.

The GMP Information Compliance and Records Management Unit can be contacted at: dataprotection@gmp.police.uk

What this Policy does

Part 2 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place in some instances, when processing sensitive personal data for General Processing.

As laid out in **Police Information and Records Management Code of Practice 2023** (PIRM 2023), the policing purpose is to:

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

With regard to Live Facial Recognition (LFR) practices, GMP's usage of the technology will fall within the Policing purpose but, on occasion, may fall outside of the DPA 2018 definition of the Law Enforcement Purpose, found at Section 31 of the Act Data Protection Act 2018.

On these occasions and often for the purposes of safeguarding, special category data processed in this specific technology is done so in accordance with the requirements of Article 6 and Article 9 of the UK GDPR. GMP's processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by GMP in our capacity as a competent authority and falls under Part 3 of the DPA and is subject to a separate APD.

Processing of special categories of personal data

Special categories of personal data are defined in Article 9.1 of UK GDPR as:

- Data revealing racial or ethnic origin,

- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data,
- Biometric data for the purpose of uniquely identifying a natural person,
- Data concerning health
- Data concerning a natural person's sex life
- Data concerning a natural person's sexual orientation.

Processing sensitive personal data for general purposes must comply with the requirements of an Article 9.2 of the UK GDPR. For the Purposes of LFR the appropriate Article 9.2 conditions are:

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

Processing under this article will be limited to processing participating staff images for the purpose of validating LFR technologies.

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

Article 9.2(g) - Processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

When relying on Article 9.2(g) a further condition must be met in Schedule 1, Part 2. These will be one or more of the following:

Para 5 Requirement for an Appropriate Policy Document (APD) – (This Document)

The requirements of the APD are laid out in paragraph 39 in Part 4 of the DPA 2018.
This condition is met when the document (a) explains the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and (b)explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.

This document explains GMP's data processing for LFR and satisfies the requirements of Schedule 1, Part 4 of the DPA (APD and Additional Safeguards). It sets out and explains GMP's procedures for securing compliance with the principles in Article 5 GDPR (relating to

processing of personal data) and policies regarding the retention and erasure of such personal data.

Para 6 Statutory etc, and government purposes

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

The police have a common law duty not only to prevent and detect crime but to protect the public and preserve life and property: this is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions. The processing is also necessary for reasons of substantial public interest, that is, the safety and protection of the public. In determining necessity GMP will always consider whether less intrusive measures can be used without compromising the objective and the interests of the individual balanced against the interests of the community.

Para 18 Safeguarding of children and of individuals at risk

This condition is met if the processing is necessary for the purposes of protecting an individual under 18 (or over 18 and at risk i.e. vulnerable for reasons defined in the paragraph 18) from neglect or physical or emotional harm or protecting the physical, mental or emotional well-being of an individual, where the consent cannot reasonably be given or obtained in the relevant circumstances, and the processing is necessary for reasons of substantial public interest.

Processing of personal data relating to criminal convictions and offences

Criminal convictions and offences personal data are defined in Section 11.2 of the DPA 2018 as:

Section 11.2. …personal data relating to criminal convictions and offences or related security measures include personal data relating to—

(a)the alleged commission of offences by the data subject, or
(b)proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.
Processing personal data relating to criminal convictions and offences for general purposes must comply with the requirements of an Article 10.1 of the UK GDPR:

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority ***or***
when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

As GMP will only process this specific personal data type under its official authority when utilising LFR technologies for a general purpose, there are no further requirements for GMP to meet the additions requirements as laid out in Section 10(5) DPA 2018.

Description of Data Processing

The Data Processing Operations related to LFR

GMP's LFR system is a dedicated CCTV system delivered via CCTV equipment on a liveried vehicle/s deployed in a static location. The technical operations of the LFR usage are documented within GMP's LFR Policy and Procedure documents.

It is clear from the technical operation of LFR that personal data is processed in relation to two classes of individuals, namely (1) those on an LFR Watchlist and (2) those who pass within the relevant LFR Zone of Recognition.

Personal data that is processed in the Deployment of LFR

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

• Subject name
• Facial image, and from/associated with that facial image:
  ○ Biometric facial image template
  ○ Recorded (or if unknown, perceived) gender
  ○ Recorded (or if unknown, perceived) age/date of birth
  ○ To the extent arising from looking at the image, any perceived religious or philosophical beliefs, perceived ethnicity, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).
• Criminal offence data or information concerning why they are missing in order to confirm why the subject is a Person of interest (which, in particular in the case of MAPPA nominals, may include data concerning the individual's sex life)
• Warning markers (e.g. known to possess weapons)
• Alert Type
• Unique Reference No. (URN)
• PNC ID
• Note: Further personal data would be available to, and recorded by officers using GMP local systems during the Engagement process. This is not data processed by way of LFR deployment itself, and is instead relevant to the conduct of officers in the normal course of their duties
	• CCTV footage of data subjects passing through the Zone of Recognition
	• Available to GMP via the use of the CCTV footage:
	  • Biometric facial image template for alerts only. Biometrics for non-alerts are deleted instantly.
	  • Perceived gender
	  • Perceived age
	  • Perceived height
	  • Metadata (i.e. location, date and time the footage was captured)
	  • Any perceived points concerning a relevant disability/gender transition
	  • On some occasions any perceived religious or philosophical beliefs, any perceived data concerning health and sexual orientation (e.g. by reference to clothing/headwear).

In respect of those on a LFR Watchlist, the data is mainly drawn from GMP's local systems. The data subjects placed onto the watchlist are usually already known to GMP, with the data already being processed in order to undertake law enforcement investigations, operations, incidents. There will be occasions where no image is held by the Force or, if one is held, where its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police-originated image. Non-police-originated should only be included in a watchlist with the authorisation of the Authorising Officer (AO). Further information can be found Watchlist | College of Policing

The process of Watchlisting a data subject creates new data as follows:
(i) the biometric facial image template to enable the operation of the LFR system
(ii) data that an individual has been placed on a Watchlist, albeit refer to Section 11 of the Policy regarding the deletion of the Watchlist following the conclusion of the Deployment.

Stage	Action
1	**Construction of Watchlist**
	A Watchlist is constructed using images of Persons of interest which are already held by GMP. The LFR software then detects and analyses the facial features shown by the images in order to then express those features as a set of numerical values (i.e. a Biometric Template).
2	**Facial image acquisition**
	The LFR cameras provide CCTV footage of those persons who appear within the Zone of Recognition in real time, as a live feed to the LFR computer system. The live feed is viewed in real time by an LFR Operator for the purposes of ensuring that the LFR system is working properly and to support Engagement Officers. The nature of the imagery which can be seen by the LFR Operator is described below in Stage 6
3	**Face detection**
	The LFR software detects individual human faces within the images captured by the LFR live feed.
4	**Feature extraction**
	The LFR software then produces a Biometric Template of the facial features of each detected face
5	**Face comparison**
	The LFR software compares the Biometric Template of the facial images of persons captured via the live LFR feed with the Watchlist Biometric Templates
6	**Matching**
	When the Biometric Templates obtained via the live feed are compared with the Watchlist biometric templates, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity between the Templates, with a higher score indicating greater points of similarity. If the score surpasses a pre-set threshold value, the LFR software will generate an Alert to indicate that a possible match has occurred.
7	**Engagement Officer consideration of matched images**
	Once an Alert has been generated, Engagement Officers who are trained on LFR use will assess the relevant Candidate Image against the relevant Watchlist image and make a decision as to whether they consider the match to be viable, and if so whether any further action is required.
8	**LFR data destruction**
	In the absence of an Alert, the biometric templates created in respect of members of the public whose images have been captured by LFR are immediately and automatically deleted. All LFR CCTV footage is deleted within 31 days of the particular LFR deployment. LFR Watchlists are deleted as soon as reasonably practicable and in any event within 24 hours.

Personal data processed in relation to those Engaged

Where data subjects are Engaged, the data gathered is not materially different to that which would occur where police were engaging with an individual, other than where prompted by LFR – for example, where an officer is engaging with a person because they match a phoned-in description of an offender, or because the officer believes the person to match the appearance of someone on a wanted poster. As the Engagement officer seeks to ascertain the identity of the Alerted person, and to validate the reason for which they are a person of interest, officers will use their normal policing powers and capabilities available to them and gather persons data associated with the use of those powers.

Personal data processed post-Alert

Section 10.4 of GMP's LFR Policy stipulates that GMP will maintain a register of Deployments. This section confirms the data that will be maintained in the register.

The retention of personal data is processed in line with Section 11.1 of GMP's LFR Policy. In particular:

a) Where the LFR system does not generate an Alert, that a person's biometric data is immediately automatically deleted by the LFR software.
b) The LFR Watchlist will be deleted as soon as reasonably practicable, and in any case within 24 hours, following the conclusion of the Deployment.
c) Where the LFR system generates an Alert, all related personal data is deleted as soon as practicable and in any case within 24 hours, except to the extent that:

    (i) Personal data is retained in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996.
    (ii) Personal data is retained in accordance with GMP's complaints / conduct investigation policies.

d) The CCTV footage generated from LFR Deployments will be deleted within 31 days, except to the extent that the footage is retained:

    i. In accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996.
    ii. In accordance with GMP's complaints / conduct investigation policies.
    iii. In accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Location and Frequency of Data being Processed

Data is processed in relation to a specific LFR Deployment, the frequency and location of LFR Deployments cannot be estimated as they will be intelligence led. See Section 10 of GMP's LFR Policy for more information around the Governance and Oversight.

The number of people on a Watchlist will vary between Deployments. Rather than being driven by the LFR system's capacity, the inclusion of Persons of interest on any particular Watchlist is responsive to the particular use case being considered for LFR Deployment.

Algorithm Accuracy

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

Data Sharing

Should the LFR system generate an Alert, the subsequent process will involve GMP's personnel using policing databases and other intelligence systems to inform any further action. This subsequent action may also involve GMP working with other police forces, law enforcement bodies, and / or other agencies to assist GMP in discharging its common law policing powers. This action will not require the sharing of biometric data but may require GMP to share personal data, as it would for any investigation, in accordance with GMP's routine sharing arrangements. The process following an Alert and any decision to share data is no different to where a person was located and identified without the use of LFR (i.e. as a result of a human-eye recognition by an officer picking out a watched subject).

Procedures for ensuring compliance with the principles in Article 5 UK GDPR

Accountability

To comply with the Accountability Principle (Article 5(2) UK GDPR) GMP have put in place appropriate technical and organisational measures. These include: -

- The appointment of a Data Protection Officer who is responsible for independent advice and monitoring of data protection matters and who reports directly to the Chief Officer team for GMP.
- Taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations
- Maintaining documentation of our processing activities and provide these records to the Information Commissioner's Office ('ICO') on request
- Adopting and implementing data protection policies and procedure and ensuring personal data is only collected, used or handled in a way that is compliant with data protection laws and have appropriate written contracts in place with our data processors.

- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out Data Protection Impact Assessment for any high-risk personal data processing and consult the ICO if appropriate.
- Record and investigate all personal data breaches and near misses.
- Review and update our accountability measures when required.

PRINCIPLE (A) - LAWFUL, FAIR and TRANSPARENT

Processing personal data under UK GDPR must be lawful, fair and transparent. Processing shall be lawful only if and to the extent that at least one Article 6.1 condition is met.

Furthermore Processing of special categories of personal data shall be prohibited, unless at least one Article 9.2 condition is met. When GMP are relying on *Article 9.2(g) - Processing is necessary for reasons of substantial public interest,* a further condition is met from Schedule 1. As described at the start of this document.

Under Article 10, Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 shall be carried out only under the control of official authority. As described at the start of this document.

Furthermore, the authority to deploy LFR in support of a policing operation will be made by an officer not below the rank of Superintendent (the Authorising Officer or AO). Their authorisation will be recorded in writing (Application / Written Authority Document). The form provides for a baseline of safeguards to ensure that the need for the Deployment and the currency of the Watchlist continues to be maintained with due oversight.

Prior to AO authorisation and the Deployment of LFR in public spaces the AO must ensure that the following assessments are reviewed and/or completed:

- Community Impact Assessment (CIA),
- Equality Impact Assessment (EIA),
- Data Protection Impact Assessment (DPIA),
- Operational Risk Assessment & Surveillance Camera Commissioner's self-assessment.
- A GMP officer of Command rank (ACC rank or above or Police Staff equivalent) must be briefed on the proposed deployment by the AO.

Whilst the senior officer does not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed deployment to an elevated level of strategic thinking. This affords NPCC the opportunity to veto the deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.

If they authorise the deployment, the AO must ensure that the following are briefed on the proposed deployment:

- An officer of the rank of Superintendent or above for the relevant District/s (if not the same as the AO) is aware of the proposed deployment, and
- The office of the Deputy Mayor for Safer & Stronger Communities
- The Duty ACC (via Force Daily Management Meeting).

The AO must have concluded not only that a Deployment is likely to achieve one of the identified policing objectives under the Policy, but also that there is no effective alternative means of achieving that objective that is less intrusive than the Deployment, and that the Deployment strikes a fair balance between the rights and freedoms of those affected by the Deployment and the achievement of the relevance policing objective.

GMP is subject to obligations under the Human Rights Act 1998. Compliance with the Policy and Procedure documents serve to ensure that Deployments are undertaken only in compliance with the 1998 Act.

GMP is subject to obligations under the Equality Act 2010. GMP has considered the equality impacts of LFR in general by way of its Equality Impact Assessment and continues to keep these under review by way of regular review. In accordance with the Policy, each Deployment will also be subject to a review of the GMP LFR Equality Impact Assessment.

Compliance with the Policy will also serve to ensure that sensitive processing is fair. In effect, fairness is built in both to the design of the Policy and the assessment process which the AO must undertake in the context of any individual deployment. The Policy requires focused consideration of the impact of processing on affected individuals, as set out above. Moreover, the assessment process required in respect of each LFR deployment obliges the AO to consider amongst other things the reasonable expectations as to privacy of affected individuals and more widely whether the deployment strikes a fair balance between the interests of data subjects and the wider policing interests served by the deployment.

GMP's LFR Documents published on GMP's website together with GMP's LFR Privacy Policy. These steps ensure privacy information is made available to the public and that GMP Deploys LFR in a lawful, fair and transparent manner.

PRINCIPLE (B) PURPOSE LIMITATION

GMP process personal data where it is necessary for the purposes of protecting the public, fulfilling our common law functions to preserve and protect life and property, and to safeguard children and vulnerable persons, all in the substantial public interest.

GMP's DPIA provides an assessment of the risk to the rights and freedoms of data subjects in relation to Principle (b) and identifies the mitigations which apply.

Section 5.3 of GMP's LFR Procedure document covers watchlist generation and the criteria for inclusion of an image on a watchlist.

Furthermore, compliance with Section 11 of the Policy (data management) will serve to ensure that sensitive data generated in the course of a Deployment is not processed in a manner that is incompatible with the purpose for which it was collected. In particular, section 11 makes provision for the deletion of biometric data, watchlist images and CCTV footage (including the immediate deletion of a person's biometric data where the LFR system does not generate an Alert in relation to that person).

PRINCIPLE (C) DATA MINIMISATION

GMP process personal data necessary for the specified purposes and ensure it is adequate, relevant and not excessive in relation to the purpose(s) for which it is processed. The

information we process is only that which is necessary for and proportionate to our purposes.

LFR deployments are subject to extensive scrutiny prior to deployment, including location and duration of a deployment. The Watchlist generation and criteria (Section 5.3 of GMP's LFR Policy) sets out restrictions and boundaries around what should and should not be used for a deployment.

As stipulated throughout, Section 11 of the policy makes provision for the deletion of biometric data, watchlist images and CCTV footage.

GMP's DPIA provides an assessment of the risk to the rights and freedoms of data subjects in relation to Principle (c) and identifies the mitigations which apply. Amongst other points, this DPIA recognises the LFR system's design has a number of data protection 'by design' features. These include:

- Immediate automatic deletion of biometrics data where the LFR system does not generate an Alert;
- The ability to manually delete a data subject from the watchlist after a True alert;
- The LFR system undertakes checks on ingestion to flag images of poor quality.

PRINCIPLE (D) ACCURACY

Inaccuracies in the data itself

GMP's DPIA provides an assessment of the risk to the rights and freedoms of data subjects in relation to Principle (d) and identifies the mitigations which apply. Amongst other points:

- Section 5.3.1 of GMP's LFR Procedure stipulates Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment. This ensures that LFR Engagement Officers are making decisions on the most current data available to them.
- A new Watchlist is generated for every LFR Deployment. This is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching. GMP personnel are required to have taken reasonable steps to ensure that the image is of a person intended for inclusion on a given Watchlist.
- The LFR system undertakes checks on ingestion to flag images of poor quality.
- Adjudication means that the decision to Engage a member of the public is made by an Engagement Officer and not the LFR system. Police officers undertake checks during the Engagement process to ascertain identify and validate the reason the person is of interest. The LFR Alert alone is not a definitive confirmation of identity.

Inaccuracies in the algorithm

GMP's DPIA provides an assessment of the risk to the rights and freedoms of data subjects in relation to Principle (d) and identifies the mitigations which apply. Amongst other points:

• GMP has paid close regard to the NIST and NPL findings and the recommended threshold settings. 5.1.1 of GMP's LFR Procedure document holds further detail.
• The post-Deployment review process provides a means by which algorithm issues can be flagged and resolved. The demographic composition of those subjects engaged with, in terms of numeric totals, and retention of the CCTV footage for a 31 day period supports analysis of Alerts.
• GMP's FR Technology Board monitors for trends, review the demographic composition of Alerts quarterly and can direct change at a strategic level in a FR context.

PRINCIPLE (E) RETENTION

LFR data processed in accordance with Part 2 DPA 2018 (UK GDPR) is subject to Section 11 (Data Management) of the LFR Policy which sets out applicable retention periods.

GMP's LFR System is also deigned to support compliance with Principle (e), and is capable of audit to ensure compliance. Key system design points are:

- Where the LFR system does not generate an Alert, the biometric data of the person passing through the Zone of Recognition is immediately and automatically deleted by the LFR system.
- The LFR system design enables GMP to delete data in line with policy and in response to individual rights requests.

GMP maintains records of processing activities in compliance with Article 30 UK GDPR.

In limited circumstances Probe Images and Biometric Templates will be used for research purposes and evaluation of the effectiveness and performance of the FRT System. Where possible personal data will be anonymised or pseudonymised. Personal data being processed for research purposes will be done so in accordance with a data sharing agreement requiring sufficient guarantees around the security of the information in transit and at rest, including physical, personnel and technical security measures. Such measures will be subject to scrutiny by Force Information Security Officers and the Data Protection Officer.

PRINCIPLE (F) 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. Furthermore, specific training is provided to officers working with LFR which is supplemented by GMP's LFR Policy and Procedures documents.

Section 11.2 of the Policy outlines applicable data security measures adopted to secure the use of LFR. The DPIA further identifies measures in relation to personnel security, training,

operational risk, security against unlawful processing and business continuity measures to protect against data loss.

Policy applicable to Retention and Erasure

GMP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with GMP's LFR Documents. This means that:

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

Where the LFR system generates an Alert, all related personal data is deleted as soon as practicable and in any case within 24 hours, except to the extent that:

- Personal data is retained in accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996;
- Personal data is retained in accordance with GMP's complaints / conduct investigation policies.

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

• In accordance with the Data Protection Act 2018, PIRM 2023 and the Criminal Procedures and Investigations Act 1996;
• In accordance with GMP's complaints / conduct investigation policies;
• In accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Appropriate Policy Document Review Date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases. This policy will be reviewed annually or revised more frequently if necessary.

Further information relating to GMP's LFR can also be found in relevant supporting documents:

- LFR Policy Document,
- LFR Procedure Document,
- LFR Legal Mandate,
- Community Impact Assessment,
- Equality Impact Assessment,
- Data Protection Impact Assessment,
- Operational Risk Assessment & Surveillance Camera Commissioner's self-assessment.

Policy document Sign-Off

Person Completing / Reviewing the APD	
Name	**Date**
Rachael Bigland	June 2025

Data Protection Officer Review	
Name	**Date**
Suzanne Martin	September 2025

IAO / Force lead Review	
Name	**Date**