Appropriate Policy Document

Live Facial Recognition (LFR)

Policy on the processing of Special Category Data Under Part 2 of the Data Protection Act 2018 and Article 9 of the UK General Data Protection Regulation (GDPR), and Part 3 Section 42 of the Data Protection Act 2018

Processing Biometric Data, for the purpose of uniquely identifying an individual.

Version 1.1

Norfolk and Suffolk Constabularies

Information Management

Version #	Implemented by	Revision date	Details
0.1	Information Management	Feb 2025	First Publication
0.2	Information Management	April 2025	Revised template
1.0	Information Management	June 2025	Amendments following consultation and deployment.
1.1	Information Management	March 2026	Amendments to remove internal links

Contents

1. Introduction

1.1. This document is the 'Appropriate Policy Document' as regards the specific sensitive processing relating to Live Facial Recognition (LFR) it adds to and supplements the Appropriate Policy Documents in place for other sensitive processing conducted by the Norfolk and Suffolk Constabularies.

1.2. Because LFR processing will be undertaken both in relation to processing for Law Enforcement purposes[1] as well as in relation to processing for other purposes (such as processing relating to the safeguarding of vulnerable persons) this document is drafted so as to meet the Appropriate Policy Document requirements of both the Law Enforcement Processing regime under Part 3 of the DPA 2018 and the general processing regime under the UK GDPR.

Part 3 DPA Law Enforcement Processing

1.3. As regards Part 3 of the DPA and law enforcement processing, in line with the requirements of s.42 of the DPA 2018 this document explains both the procedures deployed for ensuring this sensitive processing is compliant with the data protection principles and the policies in place as regards the retention and erasure of the specific personal data used in this particular context of LFR related sensitive processing.

1.4. Sensitive processing is defined in Part 3 section 35(8). This 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,

[1] As defined in s.31 DPA 2018

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.

1.5. Processing for LE (Law Enforcement) purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. Additionally, such sensitive processing can only take place where there is an Appropriate Policy Document (APD) in place and the processing is either based on consent (Section 35(4) DPA 208) or where it is strictly necessary for a law enforcement purpose and is based on a Schedule 8 DPA 2018 condition (Section 35(5)).

UK GDPR Processing

1.6. As regards the UK GDPR, in line with the requirements of Article 9 and 10 of the UK GDPR alongside s.10 and schedule 1 of the DPA 2018 2018 this document explains the procedures deployed for ensuring this processing of special category and criminal convictions and offence data is compliant with the principles in Article 5 of the UK GDPR and explains the policies in place as regards the retention and erasure of the specific personal data used in this particular context of LFR related processing.

1.7. Section 10 of the DPA 2018 requires that where the processing of special category personal data is reliant on one of the following lawful bases, as described in Article 9 of the General Data Protection Regulation 2016/679 (GDPR), the processing must also satisfy one of the points of Article 9 of the DPA 2018:

- Article 9 (b) Employment, social security and social protection.
- Article 9 (g) Substantial public interest.
- Article 9 (h) Health and social care.
- Article 9 (i) Public health.
- Article 9 (j) Archiving, research and statistics.

1.8. These conditions also require that there is an Appropriate Policy Document in place as regards the processing of special category data.

1.9. Given Live Facial Recognition involves the processing of biometric data, this is both sensitive processing under Part 3 of the DPA and processing of special category data under the UK GDPR, and therefore these requirements are engaged.

1.10. This document (the LFR APD) is complemented and supported by other wider Suffolk and Norfolk documents including the general record of processing activities[2] and the other LFR documents which includes (this list is not exhaustive):

- LFR Policy

[2] As required by s.61 DPA 2018 and UK GDPR Art.30

- LFR Standard Operating Procedures (SOP)
- Legal Mandate
- Data Protection Impact Assessment (DPIA)
- Appropriate Policy Document (APD) General Data Protection Regulation (GDPR)
- Appropriate Policy Document (APD) Part 3
- EIA

1.11. This document will remain in place from when the relevant processing begins through to a date no sooner than 6 months following the cessation of the relevant processing. This document will remain under constant review during that period and will (if appropriate) be updated from time to time as well as be made available to the Information Commissioner upon request (and without charge).

2. Applicability

Summary of the relevant proposed sensitive processing

2.1. LFR involves the deployment of police resources to a geographic location where live video footage is captured. That footage is then analysed by the LFR technology to create biometric templates of every face that appears in that footage. Those templates are immediately compared against a prepared watchlist of biometric templates of individuals selected as persons the police need to locate. Where a match takes place the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the Watchlist are presented to the LFR Operator / LFR Engagement Officer for human review. The LFR Operator / LFR Engagement Officer will consider the Alert, noting the System, Subject and Environmental Factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is engaged.

Description of Data Processed:

2.2. The data processed utilising LFR:

Biometric data for the purpose of uniquely identifying a natural person.

LFR Is a real-time deployment of facial recognition technology (FRT), which in summary compares one or more live camera feeds where the faces are isolated and processed by comparing those biometric templates against a predetermined Watchlist of biometric templates in order to locate Persons of Interest by generating an Alert when a possible match is found.

In practice this involves the following specific types of personal data:

- Live video footage obtained at the deployment location of persons who pass within the field of vision of the camera(s)

- Creation of a biometric template of each face that appears within the live video footage. From this category of data subject (i.e. those individuals that pass through the area covered by the live video feed) no other personal identifiers are collected other than the biometric template

and the video image it is derived from, unless and only where a match is identified, and further action is taken after the LFR processing has indicated a match.

- The collection and analysis of a selection of facial images of known data subjects to create a watch list. The watchlist is bespoke for every deployment and the rationale for the make-up of the watchlist must be intelligence-led, justified, proportionate and necessary, with the nature of the watchlist recorded prior to each deployment.

- Creation of a biometric template for each face of a known data subject who features within the watchlist.

- Enrolment and storage of the biometric templates created from the watchlist into the LFR system to be deployed, along with other associated metadata to identify them (such as name, date of birth, unique reference number etc).

  Where necessary criminal conviction or offence data will also be processed as part of creating the watchlist. This will be the case for example where it is part of the rationale for creating that specific watchlist. If a number of suspects are sought in relation to a particular crime that offence data would be processed as part of the justification for that particular watchlist. The criteria will vary according to the purpose of the watchlist and deployment. For example, when deploying in a certain area the watchlist could be compiled of those with bail conditions or Community Behaviour Orders preventing them from being in that area. The watchlist is reviewed as part of the authorisation process.

  Biometric data used to uniquely identify an individual is considered to be special category data. For this processing we will be collecting the personal data of members of the public which will include an image that will be utilised by extracting a biometric template from it for the purposes of uniquely identifying them.

  We maintain a record of our processing activities in accordance with s. 61 DPA 2018 and Article 30 of the UK-GDPR.

Part 3 Condition for processing

2.3. The following are the schedule 8 conditions for this LFR processing:

2.3.1. necessary for the exercise of a function conferred by an enactment or rule of law – for reasons of substantial public interest;
2.3.2. necessary for the administration of justice;
2.3.3. necessary to protect the vital interests of the data subject or another individual;
2.3.4. necessary for the safeguarding of children and of individuals at risk; and
2.3.5. necessary for the purpose of preventing fraud.

UK GDPR Conditions

2.4. UK-GDPR conditions for processing special category data:

Suffolk and Norfolk Police process special categories of personal data under the following GDPR Articles:

2.4.1. Article 9(2)(a) – explicit consent

In the limited circumstances where we seek consent, we make sure that the consent is

unambiguous, is a freely given, fully informed affirmative action which is recorded and managed to ensure the facilitation of individual rights, including withdrawal of consent. Processing under this article for LFR activities will be limited to the processing of participating staff images for the purpose of validating LFR. This will be carried out in circumstances where volunteers are asked for and where it has been made explicitly clear that there is no requirement for any staff to take part and participation will not be considered for any kind of performance or other evaluation purposes and that there will be no adverse consequences for anyone who does not want to volunteer.

2.4.2. Article 9(2)(g) - Substantial Public Interest

E.g. Identification of missing persons or safeguarding children or vulnerable individuals.

Section 10 DPA supplements Article 9 GDPR, requiring the one of the following conditions of part 2 of Schedule 1 to be satisfied where Article 9(2)(g) is relied on.

We process special category data for the following purposes identified in paragraphs 6 and 18 of Part 2 of Schedule 1 (substantial public interest conditions):

Paragraph 6 – Statutory etc and government purposes - exercise of functions conferred upon a person by enactment or rule of law. 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, both forces 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. Such a balance will depend on the context, in some cases the location of an individual might be more proportionally executed by attending their known addresses but in other cases where that data is missing or out of date, it may be less intrusive and more effective to use LFR at locations they are known to frequent. Similarly, sometimes LFR might be less intrusive that other options such as issuing mugshots to hundreds of officers and staff than to use a single discreet and secure LFR system.

Paragraph 18 - Safeguarding of children or 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 legislation) from neglect or physical, mental 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 (or the consent would prejudice the protection sought to be given), and the processing is necessary for reasons of substantial public interest. An example, but not limited to, LFR use for safeguarding of children could be locating missing children. Police can use LFR in transport hubs (train stations,

airports or bus terminals) to quickly identify missing children. Their image can be added to a watchlist allowing officers to receive alerts if the child is detected.

3. Associated Documentation

- Legislation/National Guidance
- Authorised Professional Practice (APP)

4. Compliance with data protection principles

4.1. Accountability Principle under both UK GDPR and Part 3 DPA

Suffolk and Norfolk Police have put in place appropriate technical and organisational measures to meet the requirements of accountability and demonstrate compliance with wider requirements of both UK GDPR and Part 3 of the DPA 2018 and in particular the principles. These include: -

• The appointment of a data protection officer who is ultimately responsible for data protection compliance for LFR.

• Taking a 'data protection by design and default' approach to our activities.

• Maintaining documentation of our processing activities specifically including the completion of DPIA's and Equality Impact Assessments for each deployment as well as ensuring each deployment makes appropriate entries as regards the relevant Records of Processing Activities (as per s.61 DPA 2018 and Article 30 UK GDPR), and as regards Law Enforcement purpose processing also in relation to the Log required by s.62 DPA 2018.

• Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.

• Implementing appropriate security measures in relation to the personal data we process. This is covered in the LFR Policy.

• Carrying out DPIA's for our high-risk processing at a minimum but also undertaking DPIA's wherever we think it would be helpful, appropriate and proportionate to do so.

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

4.1.1. First Principal Compliance

4.1.1.1. Part 3 Processing - Principle (1): lawfulness and fairness

Processing personal data must be lawful and fair. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing is necessary for the performance of a task carried out for the law enforcement purpose by either constabulary as a competent authority. As LFR involves sensitive processing, in addition, in the absence of consent, it is only lawful if the processing is strictly necessary for the LE purpose and the processing a) meets at least one of the conditions in Schedule 8 and b) Suffolk/Norfolk Police has in place this APD.

The processing of data by LFR is strictly necessary for the exercise of Suffolk and Norfolk Constabulary functions of preventing and detecting crime and protecting public safety for reasons of substantial public interest (see above under Conditions for processing sensitive data). Reliance will be primarily on condition 1 of Schedule 8, but conditions 2, 3, 4 and/or 8 may also apply. We have given examples of where this may be the case above. Both constabularies will always consider whether the use of LFR is strictly necessary (i.e. considering other measures not involving sensitive processing and whether they could achieve the same outcome) and will always ensure that at least one relevant condition is satisfied. There will be a very limited subset of LFR processing which relies on consent instead, this will be limited to the processing of staff images for validating and calibrating the LFR system prior to or during a deployment for law enforcement purposes. We undertake measures with the staff involved to ensure that the consent is freely given and valid otherwise such processing is explicitly prohibited.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and this policy document. The DPIA for LFR gives specific detail regarding the way in which data is processed and how the measures we have in place ensure that the processing is lawful, fair and transparent. Relevant documentation and additional information about how LFR is used will be available to the public on the Norfolk and Suffolk website(s), facial recognition section, to be created but which will be made public before any relevant processing begins.

As regards the underlying legal frameworks that apply to the activities conducted in the deployment of LFR further detail is provided in the Legal Mandate document.

4.1.1.2. Part 3 Processing - Principle (2): purpose limitation

Suffolk and Norfolk's law enforcement (LE) purposes for processing using LFR are primarily the prevention, investigation, detection and prosecution of crime but also the safeguarding against and the prevention of threats to public security. These are all LE purposes under s.31 DPA 2018.

On each occasion that LFR is used, the relevant specific and legitimate LE purpose will be explicitly recorded.

We process sensitive data using LFR when it is necessary for us to fulfil these statutory functions listed above in the substantial public interest, including where it is necessary for complying with or assisting another body to comply with a regulatory requirement, to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts. An example would be if an individual is suspected of committing a criminal offence and is therefore wanted for questioning but other routes of locating the individual have been unsuccessful and so LFR may then be used in order to fulfil the statutory function of the investigation of a crime.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other LE purposes here, 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 could instead be used, and 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.

If we are sharing data collected for LE purposes with another controller, we will ensure and document that they are authorised by law to process the data for their LE purpose and that the processing is necessary and proportionate to that purpose.

We will not process personal data for purposes incompatible with the original purpose for which it was collected.

We will not process data collected for an LE purpose for a purpose that is not an LE purpose unless the processing is authorised by law and meets the requirements of the UK-GDPR and DPA.
As regards further processing the approach will differ slightly between different types of sensitive data involved in the LFR.

A) As regards the sensitive data relating to the video feed and biometric templates derived from it at the deployment, this information is held to a short retention period, as set out in section 5. Where this relates to a particular image and/or template that does result in a match this data will potentially be further processed for law enforcement purposes related to the specific, relevant and legitimate law enforcement purpose the relevant person was added to the watchlist for, where this is necessary and proportionate.(e.g. to be included as part of the investigation file as regards an absconding prisoner as part of the evidence as to where and how they were located).

B) As regards sensitive data relating to the creation of the watchlist such as the facial image, criminal and conviction data, the biometric template derived from it and the associated other data this information will similarly be further processed as set out above where a match occurs in a deployment. However, where watchlist data does not result in a match this information may be further processed for future LFR deployments on a similar basis as the original deployment where the processing remains necessary and proportionate for the specific relevant law enforcement purpose associated with that individual (e.g. the individual is suspected of a series of violent offences and remains at large and subject to an arrest warrant so even though they didn't match on a first deployment they may be included in later deployments for the same reason).

C) The specific copies of the data used in the LFR are unlikely to be used for further processing other than in either a further LFR deployment context or as evidence/records in relation to any arrest or other activity (e.g. stop and search or interview) taking place after a match has occurred. However, the original copies of information supplied for the LFR processing into the watchlist are likely to be further processed but such source images are held under other policies and so are outside the scope of this document. For example, a watchlist may use a custody photo of an individual and a description of a criminal offence he is wanted for, the copy used in the LFR won't be further processed if there is no match, but the original might be further processed at the source for other law enforcement purposes covered by another appropriate policy document.

Whenever we are considering processing any of the sensitive data used in LFR processing for a new law enforcement purpose (whether by us or another controller) this policy requires that it is first established that the additional processing for the new lawful purpose is both 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, but with the same or lesser impact on individuals and the community.

If we are sharing data collected for LE purposes with another controller, we will first satisfy ourselves and document that they are authorised by law to process the data for their LE purpose and that the processing is necessary and proportionate to that purpose. We will not process personal data for purposes incompatible with the original purpose for which it was collected.

We will not process data collected for an LE purpose for a purpose that is not an LE purpose unless the processing is authorised by law and meets the requirements of the UK-GDPR and DPA. For LFR the biometric data of the live CCTV feed will never be re-used and the biometric data from watchlist will be deleted after 31 days.

4.1.1.3. Third principal compliance: data minimisation under Part 3 and UK GDPR

When undertaking LFR related sensitive processing and/or processing of special category data our documentation, processes and procedure (including this document and the other documents linked to within it) require that before any processing takes place it is ensured that the data processed is no more than is necessary for relevant purposes and that that data is proportionate, adequate, relevant and not excessive in relation to the relevant purpose of processing. Where the specific data is known in advance of the processing (e.g. the material that will form the watch list) this will be considered in relation to each piece of data in its own context. Where the information is yet to be captured (e.g. the video footage from the deployment) this will be assessed on the basis of the type and nature of the data expected to be processed and kept under review.

Where personal data is provided to us or obtained by us, but either is not, or becomes not relevant to our stated purposes, we will erase it. An example would be if an individual's image was captured and processed creating a match that on further enquiry turns out to be a false positive because that person was not on the watchlist in fact and not subject to an enquiry.

We are also under a continuing obligation to consider at every stage of the process whether we have the right amount and kind of sensitive or special category personal data for the purposes of this processing. This requires us to keep under review both whether we could achieve the same purpose with less of this data or by processing the same amount of data in fewer ways as well as whether we have sufficient data in terms of amounts or quality/type to achieve that aim. For example, for the LFR purpose to have effect we require the data to be of an acceptable 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 facial biometric data to compare against a database, and so where images have less than this it will be necessary to remove and replace the image used.

Finally, as regards sensitive processing and/or processing of special category data there will be periodic reviews to consider whether any of the data being processed in this context needs to be deleted or supplemented/replaced. At a minimum there will be such a review immediately prior to and immediately after each specific deployment.

4.1.2. Fourth principal compliance

4.1.2.1. Part 3 - Principle (4): accuracy

As a part of the data minimisation reviews covered above the accuracy of the data will be a relevant and fundamental consideration. Where data is inaccurate or needs refreshing, we will ensure erasure, rectification, replacement or amendment takes place accordingly and without delay. Crucially we will ensure that any data known to be inaccurate is not processed as part of a LFR deployment.

Given the limited period and specific factual context that each LFR deployment will take place within issues relating to accuracy are likely to primarily arise as regards the accuracy of the original copies of the data supplied for the watchlist, which is out of scope of this document and is covered by another Appropriate Policy Document. The source system (Athena) image will be maintained in accordance with the Management of Police Information (MOPI) guidance. 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.

The types of sensitive processing involved in an LFR deployment primarily relate to data based on facts rather than data based on opinion, but some of the latter may arise in relation to metadata associated with the watchlist information. In those circumstances accuracy is determined as regards the record of the opinion is accurate and reflects it as an opinion, not the extent to which the actual content of the opinion is accurate.

As set out in this document and elsewhere in line with the requirements of s.38(3) DPA 2018 the approach taken to LFR processing takes particular care in distinguishing between different categories of data subject. In this context the prime distinction is between the data subjects who feature within the watchlist as known individuals that the Police have a law enforcement purpose for locating and those data subjects who are unknown but happen to be caught within the video feed and momentary biometric processing of the physical LFR deployment.

The pubic get higher protection and more minimal processing because biometric data is used only for a few seconds and not stored or processed other than to match against a predetermined watchlist. The watchlist is processed repeatedly against every face in the crowd in order to find a justifiable match. Images on the watchlist are assessed by the LFR algorithm. Images below a certain quality will automatically be deleted.

Finally in the context of the LFR deployments there will usually be no transmission nor making available of any of the data relating to the relevant sensitive processing to any person or body outside of the Police force operating the LFR deployment (with exception to forces utilised through Mutual Aid because those individuals are in effect seconded and working as part of the operating force not the force that sent them). However, if a deployment does intend to transfer or make available data that was subject to sensitive processing in an LFR deployment this policy requires that a quality verification of that data takes place in line with s.38(5) DPA 2018 before that data is subsequently transferred or made available to another party. As regards the transfer or making available data that is supplied to LFR deployments for watchlist creation this is out of the scope of this document and is covered by the Processing sensitive data appropriate Policy Document.

If an individual contacts the Constabularies regarding the accuracy of their data, it will respond to such requests in accordance with Section 46 data DPA 2018. Where it is decided not to erase or rectify the, the decision will be documented.

4.1.2.2. UK GDPR Accuracy Principle

In line with general principles, the accuracy of data processed for general purposes is the responsibility of all that are processing the data, and especially those who receive and input the original information into systems to ensure, as far as possible, that it is accurate, valid and up to date. All systems have privacy by design and default embedded. To comply with accuracy principles one example of steps taken is to generate the watchlist within 24 hours of deployment to ensure the data is up to date and accurate. A further example of compliance with the accuracy principle includes images on the watchlist being assessed by the LFR algorithm. Images below a certain quality will automatically be deleted. Further general accuracy principles apply, such as the requirement of officers to raise for resolution any identified data issues.

The Constabularies take reasonable steps to ensure that personal, special category and criminal offence data, which is inaccurate, incomplete or out of date is not disclosed. Reasonable steps include quality assurance checks on data including relevancy consideration as to how old the information is. If it is discovered, after disclosure, that the data was inaccurate, then the Constabularies will inform the recipient as soon as possible. Where we become aware that personal data contained within the watchlist is inaccurate or out of date, having regard to the purpose for which it is processed, we will take every reasonable step to ensure that data is erased or rectified without delay.

If we decide not to rectify or erase it, for example because the lawful basis we rely on to process the data means these rights do not 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 who we have shared that data.

If an individual contacts the Constabularies regarding the accuracy of their data, it will respond to such requests in accordance with Article 16 of the UK GDPR. Where it is decided not to erase or rectify the, the decision will be documented.

4.1.3. Fifth principal compliance: storage limitation under Part 3 and UK GDPR

All sensitive data processed by us for the purpose of an LE purpose is retained for the periods set out in our retention schedule. All information is subject to our review retention and destruction policy. Crime related information is subject to MoPI guidance with appropriate time periods for review established.

The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated).

For images where an alert is generated, the probe image and biometric template will be deleted as soon as practicable and within 24 hours, this fits our legal obligation whilst deployment is ongoing. Our retention schedule and our information holdings are reviewed regularly and updated when necessary. Where data no longer needs to be held it will be erased or anonymised as appropriate.

The probe image and related biometric template will be automatically and immediately deleted (where no alert is generated). For images where an alert is generated the probe image and biometric template will be deleted as soon as practicable and within 24 hours. The comparison process takes a matter of seconds. After an alert is generated consideration will be undertaken by an LFR Operator.

In limited circumstances images and biometric templates will be used for research purposes and evaluation of the effectiveness and performance of FRT. Where possible personal data will be anonymised or pseudonymised.

4.1.4. Sixth principal compliance integrity and confidentiality (security) under both Part 3 and UK GDPR

The particular Personal data processed by LFR is, in light of the particular risks it presents, processed within our accredited secure computer network which is located locally within Suffolk and Norfolk Police's force area in accordance with national and local security Policies. Hard copy information is processed in line with our relevant information management policies. Data Protection Policies 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 which details the bespoke security measures being applied.

All staff receive basic data protection training must undertake annual mandatory training for managing information. Specific training is provided to officers working with LFR which is supplemented with bespoke Standard Operating Procedures.

The systems we use to process personal data allow us respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information is held. All events which take place on operational systems are recorded on our records of processing activity and on an audit log which enables identification of the action executed when it was carried out and by whom.

5. Requirement to keep records of processing activity

5.1. We will retain the image of the individual and biometric template for no longer than necessary of general purposes for which it is processed. Checks and balances of the necessity of the individual included on the watchlist will be completed prior to inclusion. The source system for the image will be maintained in accordance with the appropriate retention policy and schedule. For images where an alert is generated, the image and biometric will be deleted as soon as practicable and within 24 hours. After an alert, an LFR operator will then consider the findings.

Retention and Erasure Particular to LFR Application:

5.1.1. where the LFR application does not generate an alert in relation to an individual identified from the live feed, then that person's biometric template and probe image is immediately automatically deleted.

5.1.2. where the LFR system generates an alert in relation to an individual identified from the live feed, then all personal data (to include biometric template and probe image) is deleted as soon as practicable and in any case within 24 hours following the conclusion of the deployment.

5.1.3. Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.

5.1.4. LFR operator and engagement logs are retained in line with MOPI retention periods

5.1.5. All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- in accordance with Suffolk/Norfolk Police complaints / conduct investigation policies.

Please read the Appropriate Policy Document for more information.

6. Monitoring and Review

6.1. The policy owner remains responsible for the monitoring of this policy throughout its lifespan and is responsible for making any necessary amendments required due to changes in data protection legislation.

6.2. This policy will be reviewed at least annually by the policy owner and sooner if there is a material change in policy or approach.