Privacy Notice: Surrey Police and Sussex Police
Live Facial Recognition Privacy Notice

Surrey Data Protection Officer: **Kelly Thornton**
dataprotection@surrey.police.uk
Sussex Data Protection Officer: **Jim Collen**
DPO@sussex.police.uk

Our Privacy Notice tells you how Surrey Police and Sussex Police hold, retain, process, disclose and share the information we obtain about you in relation to deployments of the Live Facial Recognition (LFR) vans. It also explains the rights you have regarding your personal information.

The use and disclosure of your personal information is governed in the United Kingdom by UK Data Protection Legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The legislation requires organisations to process data in a fair, lawful and transparent manner. It mandates that certain information must be communicated to data subjects to ensure that they are as well informed as possible about how their data will be processed.

The Chief Constables for Surrey Police and Sussex Police are defined as the 'Data Controllers' for the purposes of the legislation and are required to ensure Surrey Police and Sussex Police handles all personal information in accordance with that legislation.

Surrey Police and Sussex Police takes that responsibility very seriously and take great care to ensure your personal data is processed appropriately to maintain your trust and confidence in the police.

What is personal data?

Personal data is any information we handle that relates to an identified or identifiable natural person. An 'identifiable natural person' is anyone who can be identified, directly or indirectly from information, including by reference to a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Our Contact Details and Data Protection Officer

The Information Management Team manages data protection compliance. We take our data protection responsibilities seriously and take great care to ensure we process your personal data properly to maintain your trust and confidence. Please contact our Data Protection Officer (DPO) if you have any questions or concerns about how we process your personal data.

Email	**Surrey**	dataprotection@surrey.police.uk		
	Sussex	DPO@sussex.police.uk		
Address	**Surrey**	Surrey Police PO Box 101 Surrey Guildford GU1 9PE	**Sussex**	Sussex Police Headquarters Church Lane Lewes East Sussex BN7 2DZ

INTRODUCTION

This Privacy Notice has been created to make it easier for you to understand what personal data Sussex Police and Surrey Police processes during LFR deployments. This should be read in conjunction with the overarching Force Privacy Notice which can be found on the respective Force website:

- Sussex Police: Privacy notice
- Surrey Police: Privacy notice

PROCESSING OF PERSONAL DATA IN RELATION TO LIVE FACIAL RECOGNITION

Sussex Police and Surrey Police will be deployed LFR vans equipped with NEC's NeoFace LFR technology to prevent and detect crime, apprehend and prosecute offenders, support the administration of justice and help protect the vulnerable. Please see the links below should you wish to know more about LFR in Sussex Police and Surrey Police:

- Sussex Police: Live Facial Recognition | Sussex Police
- Surrey Police: Live Facial Recognition | Surrey Police

LFR is a technology capable of comparing a human face from a digital image against a database of faces. LFR technology analyses key facial features and generates a digital mathematical template of these features. It then compares them against the digital mathematical template of known faces in a database, generating possible matches where both images are highly likely to be the same person. The digital mathematical template is classified as 'biometric' data which when processed for law enforcement purposes. The law therefore requires us to take extra care with this sensitive data and to ensure it is used only where necessary.

Processing data is governed by both the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations Act (UK GDPR). LFR will process personal data and special / sensitive category data as outlined in the respective force's privacy notice.

LFR compares a live camera feed of faces collected from specialised CCTV cameras against a predetermined database of images (called a watchlist) to find a possible match that generates an alert. Sussex Police and Surrey Police will deploy LFR technology for the following objectives, we may consider other uses in the future and will revise this Privacy Notice whenever we do so:

- A court has issued an arrest warrant during criminal proceedings because the defendant failed to appear in court and we have been subsequently unable to locate and arrest them.
- An individual who has been released from prison on licence but due to breaching their licence conditions have had their licence revoked and have failed to return to prison.
- Suspects of specific criminal offences that need to be located to progress the investigation into an alleged criminal offence.
- To locate high risk missing persons that are believed to be at risk of, or to pose a risk of, serious harm or threats to life.

The watchlist is composed of images already held by the police, of persons who have been previously arrested on suspicion of committing an offence. On occasion, the image may have been sourced from outside of Sussex Police and Surrey Police such as provided by a family member to locate a missing person believed to be at risk of, or pose a risk of, serious harm. The watchlist of images is created within the 24 hours before each LFR deployment and the persons included are specifically selected according to the objective that a particular LFR deployment is expected to address.

The geographical area where LFR is deployed is called the 'recognition zone'. This is where the LFR police vans hosting the live cameras will be set up to scan the faces of people passing through the recognition zone. The recognition zone will be clearly marked with signage ahead of the start of the zone so that persons can take an alternative route if they wish to do so.

Leaflets and / or QR codes at the recognition zone will allow people to access more information about LFR if they choose to do so. Sussex Police and Surrey Police will publish any planned use of LFR on its website ahead of any deployment.

For each separate deployment of LFR we will carefully consider the privacy intrusion and impact on other rights of persons passing through the recognition zone to ensure it is at a proportionate level to the societal benefits of using this technology in a targeted way to prevent and detect crime, apprehend and prosecute offenders, support the administration of justice and protect the most vulnerable. Sussex Police and Surrey Police will only use LFR technology when other less privacy intrusive capabilities have not been successful or where we have strong reason to believe they would not be successful.

The LFR cameras at the recognition zone stream facial images through the LFR software. These images are compared against the images on the watchlist. When the LFR system finds a likely match an alert is generated. An officer then compares the two images side by side to establish whether they believe them to be the same person, and if so, they then decide whether to recommend that another officer speaks to the person (with that officer also exercising their independent judgement). We will always explain why we have chosen to speak with someone and give them an information leaflet with contact details if they have further questions or concerns, body worn video will also be active during the interaction.

The generated digital mathematical template of persons passing through the recognition zone will be deleted in less than a second where there has been no flagged match to a person in the watchlist.

In the future Sussex Police and Surrey Police may decide to carry out statistical research to analyse and develop the accuracy, efficacy and equitability of our use of LFR systems. Any processing of images and biometric templates via LFR for this reason would not involve the need to identify or locate persons, only to analyse the accuracy of LFR facial matching. Such research would be subject to the additional safeguards required in section 19 of the DPA 2018 and article 89 of the UK GDPR, such as anonymisation, pseudonymisation and appropriate technical security measures.

What types of personal data will LFR process?

Categories of data:

- Watch list: this uses digital custody or other images with limited identification details.
- Recognition Zone / live camera feed: digital images of data subjects.
- Records / logs of LFR deployment: metrics of number of faces scanned, alerts, interventions and arrests (non-personal data), details of police officers on LFR deployment.
- Arrest: for any alerts resulting in a person being located and arrested, details will be recorded in the Force Crime database.

Categories of data subject:

- Watch list: persons wanted on court warrant, recalled to prison, outstanding suspects of specific offence, high risk missing persons.
- Recognition Zone / live camera feed: data subjects of any age who are in the deployment area and walk through the recognition zone.
- Deployment - Police Officers and LFR system operators.

What is the purpose and intended processing?

Sussex Police and Surrey Police has a common law duty to prevent and detect crime, as set out in the 'law enforcement' in the Statutory Code of Practice on Police Information and Records Management:

- Protecting life and property.
- Preserving order.
- Preventing the commission of offences.
- Bringing offenders to justice.
- Any other police duty or responsibility arising from common or statute law.

More specifically Sussex Police and Surrey Police may use LFR to locate:

- Persons wanted under a court issued arrest warrant.
- Outstanding suspects of specific criminal offence types.
- An individual who has been released from prison on licence but due to breaching their licence conditions have had their licence revoked and have failed to return to prison.
- Missing persons believed to be at risk of, or pose a risk of, serious harm (threats to life).
- Research and analysis into accuracy, efficacy and equitability of LFR.

What are my rights under the DPA?

You have the following rights under the DPA 2018:

- Right of access to your personal data
- Right of rectification of your personal data
- Right of erasure of your personal data or the restriction of its processing
- Right to lodge a complaint with the information commissioner
- Right not to be subject to automated decision making.

Persons included on the watchlist because they are a missing person at risk of, or poses a risk of, serious harm will enjoy equivalent rights as listed above, but under the UK GDPR plus the below additional right:

- Right to object to the processing of your personal data.

The operation of LFR technology does not involve any automated decision making. Where the LFR system alerts to a potential match, the two images are reviewed side by side by the LFR system operator. Where the LFR Operator believes there is a match they pass it to a Officer who will make the decision on whether to engage with the individual.

Full details of how to exercise your rights can be found on the respective Force website and under the Privacy Notice.

What is the legal basis for processing my personal data?

Personal and Special category / Sensitive data will be processed under the UK GDPR (specifically for high risk missing persons) and Part 3 of the DPA 2018 for Law Enforcement purposes. The below list of potential processing covers all potential data processing.

- Personal Data (Article 6 (1) of the UK GDPR):
  - (e) Public task: processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  - (d) Vital interests: processing is necessary to protect someone's life.

- Special Category Data (Article 9 (2) of the UK GDPR) to include Article 10 (Criminal Data):
  - (c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
  - (g) processing is necessary for reasons of substantial public interest (see below for the conditions), on the basis of Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The following conditions apply to this processing:
    - Administration of justice and parliamentary purposes
    - Preventing or detecting unlawful acts
    - Safeguarding of children and individuals at risk (as defined at Section 18 of Schedule 1 DPA 2018)

- Lawful basis for processing sensitive data for law enforcement purposes:
  - Sussex Police and Surrey Police will process Personal / Sensitive Data under Police's legal functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The definition of a function for 'law enforcement purposes' covers activities that are for the 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
  - In addition, the police will only process sensitive data under Part 3 of the UK GDPR where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8, Part 3 Data Protection Act 2018 namely:
    - Judicial and statutory purposes/administration of justice; the sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities. In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.
    - Safeguarding of children and of individuals at risk; this condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest and is to protect them from harm or to protect their well-being.

Signs publicising the use of LFR will be prominently placed in advance (both outside and within) the zone of recognition. This measure is to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the zone (policies relating to the location of deployments also require that there will always be an alternative route to enable such a choice).

The public will be notified in advance of the Deployment without undermining the objectives, details of the LFR are to be notified to the public using force websites and other appropriate communication channels (potentially including social media).

Any member of the public who is subject to an engagement following an LFR alert should, in the normal course of events, also be offered information about the technology. Documents will be available to the public and they will be advised of the URL for the Force website and relevant pages

How long will my personal data be retained?

Watchlist:

- The images that populate the watchlist will usually be copies of those already stored in our source systems. The images in the source system will be retained in line with retention framework set out in the College of Policing Authorised Professional Practice on Information Management:
- Review, retention and disposal | College of Policing (APP). Only images lawfully retained will be drawn from the source system for the purposes of LFR.
- The copies of images on the watchlist and the biometric templates will be removed from the LFR system and any removable media used to transfer them within 24 hours of the conclusion of the deployment.
- A list of metadata of persons who were on the watchlist, (but not the watchlist images/templates), to allow sufficient time to process data subject's rights requests and for legal purposes in the case of complaint or challenge.

CCTV Footage / Live Camera Feed:

- CCTV footage recorded throughout deployment will be retained for 24 hours.
- For images and facial templates used to compare to the watchlist, if there is no match then it will be deleted instantly. If there is a match, then it will be deleted within 24 hours of the conclusion of each deployment.

How you can complain

The Information Commissioner's Office (ICO) regulates the processing of personal data. You can complain to the ICO if you are unhappy with how we have processed your personal data.

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
Information Commissioner's Office website

Date of last update and changes

We last updated this privacy notice on 22/09/2025. We keep this privacy policy under regular review and update it if any of the information in it changes