Live Facial Recognition (LFR) Technology: Legal Mandate

Summary: Outlines the legal basis for the Surrey and Sussex Police Forces use of LFR Technology

Name of Force	Surrey / Sussex Police (SY/SX)
Subject	Live Facial Recognition (LFR)
Summary	Outlines the legal basis for SY/SX's use of overt LFR technology to locate persons on a Watchlist
Author	Ch Insp [redacted]

Project Name	Facial Recognition Technology
Senior Responsible Officer-	
Business Area/Department	
Proposed implementation date	Immediately

Version	Date	Authority	Evidence of approval	Record of change
0.1	16.05.2025	Project Lead	Ch. Insp [redacted]	Initial Draft
0.2	13.06.2025	Programme Director	Det. Ch. Sup [redacted]	First Review
0.3	24.06.2025	Project Lead	Ch. Insp [redacted]	Minor Amendments
1.0	10.10.2025	SRO	ACC [redacted]	No Amendments

Contents

Terms & Definitions: Capitalised terms used in this Surrey and Sussex Police LFR Legal Mandate shall have the meaning given to them in the LFR Policy Document unless otherwise defined in this Surrey and Sussex Police LFR Legal Mandate.

1 Introduction

1.1 The College of Policing has published Authorised Professional Practice which provides guidance for the overt deployment of live facial recognition technology to locate persons on a watchlist. Surrey and Sussex Police follow this nationally agreed approach.

1.2 Surrey and Sussex Police are separate legal entities and therefore will have separate controllers doing all processing through their own Neighbourhood Policing procedures. Policies and procedures for Surrey and Sussex Police are written in a joint force manner for purposes of consistency, but each force has separate governance in place.

1.3 This document is accompanied with a Data Protection Impact Assessment (DPIA), and an Equality Impact Assessment (EIA) and dedicated Force policy.

1.4 Live Facial Recognition (LFR) for law enforcement purposes is not yet subject to primary legislation. LFR is instead regulated by several sources of primary and secondary legislation as well as both national and local policy. This 'tapestry' of legislation combines to provide a multi-layered legal structure to use and regulate the use of LFR. Below is a list of those relevant for LFR.

Tier one: Legislation	Legal Power to use LFR	a) Common Law b) Police and Criminal Evidence Act 1984 Code D (revised)
	Regulating the use of LFR	**Operational** b) Human Rights Act 1998 c) Equality Act 2010 **Data Management** d) Data Protection Act 2018 (Part 3) e) UK General Data Protection Regulation f) Protection of Freedoms Act 2012
	Requests for Information in relation to LFR	g) Freedom of Information Act 2000 h) Data Protection Act 2018 (Subject Access Requests)
Tier Two: Code and Guidance	Regulating the use of LFR	a) Surveillance Camera Code of Practise. b) Guidance issued by the Biometrics and Surveillance Camera Commissioner (Facing the Camara) c) Information Commissioner's Office Code of Practise for Surveillance Cameras and associated guidance issued by the Information Commissioner
Tier Three: SY/SX	Regulating the use of LFR	a) SY/SX Policy Document b) SY/SX Standard Operating Procedures

LFR Documents		c) SY/SX Training Documents d) SY/SX Data Protection Appropriate Policy Documents e) Data Protection Impact Assessment f) Equality Impact Assessment g) Community Impact Assessment h) SY/SX Legal Mandate

2 Common Law

2.1 The police have several long-established policing responsibilities and powers derived from common law which have been recognised by the courts. SY/SX is obliged to comply with common law and statutory safeguards in delivering its policing operational duties and they each rely on the common law to discharge several of their duties.

2.2 Key common law powers SY/SX may rely on when utilising LFR technology include the policing common law powers to:

a) protect life and property.

b) preserve order and prevent threats to public security.

c) prevent and detect crime.

d) bring offenders to justice; and

e) uphold national security.

Example: SY/SX has detailed uses of LFR as a policing tactic for locating those who are wanted for an outstanding warrant. In this context the use of LFR technology to facilitate officers to promptly locate those evading arrest would enable SY/SX to discharge its responsibilities to protect life and property. It would also be compatible with SY/SX's duty to bring offenders to justice by facilitating a prompt and effective investigation.

2.3 The use of SY/SX's common law power as a legal basis to support the deployment use of LFR has been considered and recognised in the 'Bridges' case:

a) R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (the "High Court Bridges" decision); and then on appeal in,

b) R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision).

The Court of Appeal further summarised the legal basis in relation to compilation of watchlists as being "both authorised under the Police and

Criminal Evidence Act 1984 and within the powers of police at common law." The reference to the 1984 Act is a reference to imagery obtained pursuant to Section 64A (*Photographing of suspects etc.)* of the Act and particularly section 64A(4)(a) which allows a photograph taken under the section to be "used … for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence". The Court of Appeal notes that "this was not an issue which we have to address in this appeal, since it is now common ground that South Wales Police do have the power to deploy [LFR]."

Authorising Officers: When considering the use of LFR technology, it must be clear as to the common law policing power or powers that is/are relied upon for lawfully authorising the use of LFR and why it/they apply in relation to the specific context of each proposed deployment. All of which will be recorded as part of the decision-making process.

Police and Criminal Evidence Act 1984

2.4 Section 64A of PACE allows photographing a person who is detained at a station.

2.5 Section 64ZN provides the basis such photographs to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

2.6 It is likely that in relation to LFR processing for the Law Enforcement purposes (i.e. not safeguarding purposes) the primary source of images for the creation of watchlists for LFR Deployments comes from the National Custody Database. When using such images for the purposes of creating watchlists and the associated biometric templates for those images it is therefore necessary to ensure that the purpose of using those images in any deployment meets one or more of these permitted use cases.

3 Human Rights Act 1998

3.1 SY/SX use of LFR must follow the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life (amongst others). This provides:

> ' *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*.'

3.2 As a qualified right, any interference with an individual's Article 8 rights because of LFR activity is only permissible if:

a) there is a legal basis for the interference with the qualified right that the public can understand.

b) the use of LFR (which creates the interference) seeks to achieve a **legitimate aim**.

c) Carrying out the LFR in the manner proposed is necessary for the purposes of that aim in a democratic society; and

d) the use of LFR is proportionate to the legitimate aim being sought.

3.3 It is well-established that the reach of Article 8 can be broad. The case of S and Marper v. United Kingdom[1] confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that LFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".[2]

3.4 The High Court and Court of Appeal Bridges cases considered Article 8, specifically in the context of LFR technology and confirmed that Article 8 is engaged in so far as someone passes through the Zone of Recognition and in so far as someone is placed on a LFR Watchlist for a Deployment. Depending on the nature of the deployment, the Surveillance Camera Commissioner has identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. Authorising Officers can contact SY/SX Special Legal Casework should they believe, a proposed deployment may have wider human rights point to consider. Authorising Officers are required to consider each deployment for HRA issues and potential concerns. The decisions will be documented as part of the authorising process, with specific attention being given to the use of LFR when sensitivities exist at locations such as protests, religious events, schools and hospitals as examples.

3.5 **There is a legal basis for the interference with the qualified right, that the public should be made aware of in our documentation for LFR.**

LFR will be used to allow the SY/SX forces to discharge their well-established operational duties pursuant to common law. The courts have recognised that when considering whether there is a sufficient legal basis to justify an interference as potentially being legitimate then "the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them".[3]

In the case of R (Catt) v Chief Police Officers [2015] A.C. 1065, Lord Sumption recognised that individuals could have their personal information noted down and retained by the police as they occupied publicly accessible space where it was in accordance with the law. The court recognised the police's common law powers to

[1] *(2009)* 48 EHRR 50 *at [66 and 67]*
[2] Ibid at [104]
[3] R(Catt) v Association of Chief Police Officers [2015] A.C. 1065 at [11]

collect and store information are subject to an "intensive regime of statutory and administrative regulation" under the Data Protection Act and various guidance documents on the management of police information.

The courts have further recognised the right of the police to make use of a photograph of an individual. This can be for the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. Alternatively, it can be for non-law enforcement purposes relating to safeguarding duties such as regards the location of missing vulnerable persons. It has been recognised that such purposes are not limited regarding images of just the person sought but can be extended to others such as a suspect's accomplice or of anyone else. The court confirmed the key thing "is that they must have these and only these purposes in mind and must … make no more than reasonable use of the picture in seeking to accomplish them".[4] It is well established that the reasonable and proportionate use of pictures is justifiable when pursuing such purposes and will often be of value when trying to locate persons.

3.6 In the case of the SY/SX's use of LFR, the LFR Legal Framework outlines the legal basis for any interference with an individual's Article 8 rights. The High Court Bridges case confirmed the police's common law policing powers to be "amply sufficient" in relation to this type of use of LFR and confirmed that "the police do not need new express statutory powers for this purpose". This was further considered in the Court of Appeal Bridges case which also recognised the sufficiency of the legal framework, noting:[5]

> "the legal framework which regulates the deployment of [SWP use of LFR] does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined."

3.7 In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that Police officers had in relation to the LFR deployments concerned as to their ability to determine where they deployed facial recognition technology and to determine who the deployment was intended to locate (i.e. who would be put on the watchlist). The court refers to these as the "Who Question" and the "Where Question".

a) The 'Who' Question: The Court of Appeal made it clear that, the law does not (in terms of foreseeability and accessibility) require that specific confirmation should be provided as to who each person is on a Watchlist (they recognise the Neither Confirm nor Deny (NCND) principle.[6] Rather, they recognised that individuals could be added to a Watchlist based on any valid and lawful purpose where it is fair, proportionate and appropriate to do so (such as a law enforcement purpose that they are wanted on suspicion of an offence or wanted on warrant or alternatively such as for a safeguarding purpose in relation to vulnerable persons). The consequence being that accessibility and foreseeability can be provided by knowledge that persons falling

[4] Per Laws J in *Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804 at 810F*
[5] At [69]
[6] R (*Bridges) v THE CHIEF CONSTABLE OF SOUTH WALES POLICE [2020]* At [95]

within a particular justifiable class (e.g. those wanted on warrant) will fall within scope of the watchlist.

b) Whilst it is not necessary to disclose the specific name of every individual on each watch list to satisfy the "who" question, it is also clear that for a category or class to satisfy that test it must be clear and sufficiently specific. The Court of Appeal held that a category of those "other persons where intelligence is required" was not accessible and foreseeable and so did not meet the 'in accordance with the law' test. They noted that the category was not readily understood, nor was it objective – it left "too broad a discretion vested in the individual police officer to decide who should go onto the Watchlist". It allowed police officers to decide what 'other persons where intelligence is required' meant on a case-by-case basis rather than deciding if a subject met the criteria set out in the force policy and whether the subject was appropriate in the context of all the relevant circumstances of the deployment (because for example there is no reason to believe that the subject might possibly be at the location of the deployment).

c) Following the direction of the Court of Appeal[7], SY/SX addresses the 'Who Question' in its published SY/SX LFR Documents, particularly at Section 6 of the SY/SX SOP. SY/SX sets the criteria that applies to govern the images that may be included on a watchlist and in what circumstances, deliberately circumscribing and setting the limits of the discretion to ensure the watchlist criteria is accessible and foreseeable. SY/SX explains terminology such as 'presenting a risk of harm' and 'otherwise of interest to the police' such that they can be readily understood and objective to both officers and the public. It sets out the standard required for inclusion on a watchlist, linking the necessity and criteria for the inclusion on a watchlist with the policing need and the proportionality of taking any action (always considering the context of the specific circumstances of the deployment).

d) The 'Where Question: The Court of Appeal noted that in the case before them the Police Force "was not able to draw our attention to anything which specifies where LFR Locate may be deployed". In contrast the SY/SX LFR Documents provide significant provisions that directly answer this question, particularly the SY/SX LFR SOP at Section 5. In many instances the need to locate a particular person or group of persons will determine where it is best to site LFR to facilitate making a successful location. However, other factors will also be relevant, and these include the nature of the site itself from a privacy perspective, those passing the site, and the policing need to be at the site (including for the public's protection, suppressing

[7] R (*Bridges) v THE CHIEF CONSTABLE OF SOUTH WALES POLICE [2020] At [118]*

crime hotspots, and getting ahead of crime trends). The context of the site itself as well as the date and time of day will need to be considered both objectively and as regards the watchlist proposed (both in terms of content and purpose). For example, an LFR deployment seeking to identify persons breaching a Football Banning Order could legitimately be located at a Stadium location and arguably would be inappropriate at some other location not covered by the orders. Similarly, the policies require officers to consider wider potential impacts such as where an LFR deployment for outstanding arrest warrants on a high street might unjustifiably infringe the rights of individuals because the zone of recognition effectively monitors the only entrance to a place of worship.

With the benefit of the Bridge's decisions, the law has now been applied to the live use of facial recognition technology. These judicial decisions, taken together with the SY/SX's published documentation to support the use of LFR allows the LFR Legal Framework principles to be predictably applied to the use of LFR in an accessible and understandable way. It allows the public passing an LFR system and those who may be placed on a watchlist to understand the standards SY/SX operate to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR watchlist.

3.8 The use of LFR seeks to achieve a legitimate aim

Article 8 recognises action in the interests of national security, public safety and the prevention of disorder and crime as legitimate aims. The use of LFR by SY/SX will, in line with the requirements of the LFR documentation, always be for a purpose that meets one or more of these aims. For example, this may be for the law enforcement purpose of preventing crime through using LFR to locate wanted violent offenders.

The means by which SY/SX may use LFR will be an operational decision within the parameters of the law and the SY/SX LFR documents. It will need to be driven by the policing issue at hand. This may vary from the need to locate those wanted in connection with criminality or otherwise pose a risk of harm, to more preventative tactics designed to bring reassurance to communities and enable the use of precision technology to more proactively focus policing resources. It may also be the case that a single deployment serves several compatible purposes such as where the deployment watchlist is in part relating to the locating of persons with outstanding warrants and is in part in relation to locating vulnerable missing persons and additionally the deployment of the LFR system itself serves the purpose of deterrence and visible policing (regardless of the watchlist context).

Authorising Officers: At the point that it is decided to deploy LFR, the decision maker must be clear as to its purpose(s) and how using LFR will help SY/SX realise a legitimate aim. In deciding if the use of LFR is a suitable way to achieve a legitimate aim, the decision maker must consider if benefits of using LFR justify its use for the legitimate aim when compared to any impact on the individual's Article 8 (or other) Rights. The decision maker must consider whether there are any

other ways to achieve that same aim in a way that poses less interference.

3.9 The use of LFR is necessary for the purposes of that legitimate aim in a democratic society

LFR will be used in response to a pressing social need by helping SY/SX combat crime in areas and contexts where LFR has the greatest potential to assist. It is a tool that helps SY/SX to discharge its operational responsibilities, primarily to help prevent and detect crime and protect the most vulnerable.

Authorising Officers: When considering the deployment of LFR, its use is to be underpinned by an intelligence case to highlight the need to combat the relevant crime or public safety issue or policing need to deploy and how that relates to the context of the specific deployment proposed. Having identified a need, this will allow the Authorising Officer to consider the use of LFR. Authorising Officers must decide the use of LFR is necessary and not just desirable to enable SY/SX to achieve the relevant identified legitimate aim(s). In deciding the use of LFR to be necessary, the specific issue which LFR was intending to address and how LFR would be deployed to address that problem will be documented by the Authorising Officers for each deployment. Additionally Authorising Officers must also consider and document whether the deployment was necessary in terms of whether the same result could be achieved in another more proportionate way or not.

The following are examples of why LFR may be used as a necessary tool to assist SY/SX in preventing crime and disorder. The examples are illustrative only and there will be other scenarios where the use of LFR is justified.

Personal property theft: The use of LFR will assist SY/SX in fighting criminals targeting potentially young and vulnerable persons at music events. By way of example LFR could be deployed at music venues, LFR can act as a tool to assist police officers identify those persons who are wanted and liable for arrest in connection to large scale personal property theft. LFR could have a watchlist that can be scoped to focus on traveling criminals who follow bands across Europe with the sole purpose of engaging in criminal activity and that are liable to be arrested on sight. Using LFR in this way would help SY/SX achieve its aim of preventing and detecting crime and disorder and protecting the public through the disruption and deterrence of those seeking to commit thefts by making it more difficult to enter the location. Additionally, as regards any such wanted person who was identified and stopped this would help achieve the aim of SY/SX to investigate criminal activity.

Child sexual abuse: The use of LFR will assist SY/SX in tackling child sexual abuse. LFR could be deployed based on intelligence to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse. Missing persons investigations use significant police resources where the need to locate is time critical. In such circumstances, it is of great importance to use all reasonable measures, to have the best chance of making a successful identification when the often-scarce identification opportunities arise. At times, the police may also enlist the public to help with locating missing people using public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside

of police control when it is placed in the public domain. Where it might be viable to use LFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers SY/SX a route to discharge its common law responsibilities to protect life.

However, it should be noted that data protection law is not a barrier to information sharing.

Additionally, in a climate where police forces need to operate efficiently, SY/SX has also identified that technology such as LFR can assist with the challenges of quickly and cost effectively locating those with outstanding warrants or who have otherwise breached their bail conditions. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances. The High Court Bridges case supports that there is a "considerable additional benefit to the public interest to including those wanted on a warrant" for a deployment of LFR, even when there is no specific intelligence to place them around the deployment (providing there is nothing that indicates to the contrary). The intrusion to those passing the system is no greater, but (i) the potential to protect the public from those wanted by the courts, and (ii) the positive results from such deployments where those with outstanding warrants were included in terms of progressing prosecutions (especially where other methods have failed) justified the inclusion of those with outstanding warrants from the courts as a *necessary* action to bring offenders to justice and prevent further crime, disorder and harm to others.

3.10 The use of LFR is proportionate to the the legitimate aim being sought

When considering the deployment of LFR, the benefits of using LFR for an investigation or operation should not be disproportionate or arbitrary. In this respect the Surveillance Camera Commissioner recognises that:

> *"Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".*

In this respect, the following factors (amongst others, depending on the nature of the deployment) will guide Authorising Officers:

a) *The use of LFR should be a reasonable use of SY/SX powers - it will not be proportionate if the proposed use of LFR is excessive in the overall circumstances of the investigation, operation or wider operational strategy to tackle a policing issue.*

Authorising Officers will need to consider the seriousness of the policing issues at hand and the potential benefits of using LFR and balance this with any wider impact its deployment may have to those on a Watchlist and the public at large. This will allow a decision to be made as to whether LFR is appropriate for use. Authorising Officers must consider the composition of the watchlist compiled for the LFR system to match against, to ensure that it is not compiled in an excessive or otherwise inappropriate manner. The watchlist needs to satisfy the necessity and proportionality test and will therefore be driven by the

intelligence case and bespoke for each deployment of LFR to ensure it meets the aims of each deployment.

All aspects of a deployment must be considered against this principle in particular including whether the size and nature of the watchlist is reasonable and proportionate against the stated aims of the deployment, as well as whether the location and timing of the deployment is appropriate given the aims and the makeup of the watchlist. Officers must take care never to simply reuse watchlists or other operational decisions in relation to deployments, they must be content each time that the use is reasonable and proportionate and that may require the tailoring, adjustment or entire replacement of previous similar deployment decisions to reflect the context of the next one proposed.

The watchlist compiled for each deployment of LFR should be current; based on those currently of interest to SY/SX and/or wider UK law enforcement to mitigate the risk of the LFR system matching with those no longer of interest to SY/SX and/or wider UK law enforcement.

b) Consideration should be gives as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference.

The use of LFR should be considered against other methods of locating persons of interest to SY/SX and/or UK Law Enforcement and other policing tactics which may help tackle the policing issue at hand. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation or deployment.

But it is also important to note that proportionality is not a one-way consideration that will only ever argue against the use of LFR, it can also argue in favour of deploying LFR over other methods. Officer will need to carefully consider whether other proposed methods of location would in fact be less proportionate and so be ruled out when LFR is available as an option. For example, it may be that a manual human led operation to locate a large number of individuals is ruled disproportionate because of the number of officers that the identifying information would have to be shared with in less secure contexts such as hard copies of photos, when the secure and strictly closed/limited LFR system could achieve the same aim in a more proportionate manner.

This consideration around the extent of any proposed interference with privacy against what is sought to be achieved is considered by the Authorising Officer in setting the criteria for individuals to be included on the watchlist, with each criteria having to be justified and therefore the proportionality of proposed interference is considered against the legitimate policing aim carefully and in a measured way for each deployment. This will for example ensure that in creating a particular criterion (such as persons wanted on a warrant),

consideration is given as to whether other methods have been or should be tried first. There would of course be no point in seeking to locate a missing person with a visit to their home address, but in some other cases that may be a more proportionate first step before use of LFR.

Example: Circulating a wanted image on social media may be considered as an alternative to the use of LFR.
The use of LFR can be targeted to a specific area and does not result in the public being made aware of the identity of a person being sought by the SY/SX. It can also be used for a limited period, targeted, based on wider intelligence, to times and places when it might be most expected to locate an individual.
By comparison, social media results in a person's image being put into the public domain in a less targeted way. Once online, the image is public and SY/SX no longer has control of that image. It therefore has potential to remain online even when the person has been traced and thus is a greater intrusion into the privacy of the individual being sought.
The Authorising Officer considering the use of LFR should balance any intrusion into privacy against the need for the investigative activity. If the Authorising Officer uses LFR in a way which minimises any impact it may have on a person's privacy as far as possible, it may offer a more appropriate, less intrusive alternative to a social media

c) How and why the methods adopted will cause the least possible interference to the person(s) sought and others must be addressed.

All uses of LFR under this Legal Mandate will be overt. This will include clear signage on the vehicles as well as additional signage relating to the area of deployment (such signs must always be visible at a distance that allows individuals to take action to avoid the zone of recognition). There will be uniformed officers at the deployment and there will be supporting information either published or made available online. LFR will be used for a limited time – with a limited footprint, with a defined purpose (controlled by way of the requirements of the SY/SX LFR Documents). The LFR system will be visibly deployed in an open and transparent way. Consistent with the principle of engaging with the public, the SY/SX LFR Documents also provide a structure for awareness measures which respond to the nature and objectives of the use of LFR.

Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record what other methods, as appropriate, were either not implemented or have been employed but which were assessed to be insufficient or inappropriate to fulfil SY/SX's aim.

Proportionality controls. Controls are also designed into the LFR system and its operation to help minimise any impact on the public and those placed on a watchlist as follows:

a) LFR cannot be used to locate persons unless they have been included on a prepared watchlist. Any deletion, change or addition becomes a new watchlist and will go through a further authorising process.

b) The creation of any watchlist is specific to the deployment of LFR and informed by the intelligence case for the deployment; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching.

c) Images on a Watchlist will be lawfully held by SY/SX or any other source prior to it being processed for LFR purposes with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given watchlist.

d) Authorising Officers need to expressly consider and approve the use of non-police or non-national security body originated images on any watchlist. This is because privacy considerations may attach to an image where it originates from outside of a policing or national security context. For example, it may be that the image was not placed in the public domain, was taken in a place that attracts a higher expectation of privacy or is an image that was supplied to, or taken by a third party for a specific purpose that does not usually see routine data sharing with the police. Even when SY/SX can lawfully process the images, the need for the watchlist to be a proportionate policing response requires the Authorising Officer to undertake a careful assessment of an individual's privacy expectations against the policing need to locate them using LFR (both in relation to the context generally as well as in relation to the source of the specific image). The SY/SX LFR SOP outlines considerations for Authorising Officers at Section 6.

e) On adding an image to the watchlist the LFR system will assess the image for quality and suitability for matching to allow SY/SX personnel to consider and manage the risk of poor-quality images generating inaccurate LFR alerts. This will include things such as assessing the image to ensure a clearly detectable face and facial landmarks are visible, enforcing minimum resolution thresholds of the image (i.e. if below certain pixels it will be rejected), and assessing for obstructions to the face. Whilst the system allows for manual override this will rarely be advisable.

f) All watchlists and the data they contain (including images and biometric templates) are deleted as soon as

practicable, and in any case within 24 hours following the conclusion of the deployment. To the extent that such data is a duplicate of data held elsewhere for purposes other than the watchlist, that source data will remain on the source systems it was originally drawn from (e.g. original photo, name, offence etc.) in line with current retention periods which apply to such data regardless of the deployment or not.

g) Minimum technical standards are set at the minimum threshold for the technology setting to be utilised during a deployment and is aligned with the LFR Policy. The LFR Policy currently stipulates a setting will be equal to or above the value where no FRT System bias is detected (0.64 with the current FRT algorithm). The cameras used in the LFR system are of sufficient quality for the LFR system's needs. This minimises the possibility of false positives and false negatives and is set out in the research from the National

h) The LFR system is 'closed' and not connected to other SY/SX systems or the internet.

i) The LFR system is designed to assist SY/SX personnel locate people. The LFR system will always flag potential matches to an operator for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.

j) LFR deployments and the materials that support LFR deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

Controls have also been implemented with regards to personal data retention to minimise the impact on the wider public and those on the watchlist. The controls provide that:

a) Where the LFR system does not generate an alert, then any biometric data that was created from the live feed and used to compare to the watchlist is immediately automatically deleted during the deployment. In effect this means that the system operates on a rolling basis as regards the live feed. Faces are identified in that feed, biometric templates are then created, those are compared to the watchlist and where there is no match they are then immediately deleted. The process then repeats with the next face identified in the live feed

b) In contrast where an image and a biometric template

generated from the live feed does generate an alert. That data will be retained for slightly longer in that it will be referred to the operator for review and potential further action. Nonetheless all such personal data is still deleted as soon as practicable and in any case within 24 hours following the conclusion of the deployment.

c) The data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.

d) Watchlists including the biometric templates associated with them are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment. Unlike the images and biometric templates generated from the live feed that only need to be processed for a discrete period within a deployment to determine if there is a match, the watchlist data of course needs to be held and processed throughout the entirety of the deployment because this is the data which needs to be checked against for matches in each case.

All CCTV footage generated from LFR Deployments is deleted within 24 hours, except where retained:

a) In accordance with the Data Protection Act 2018, Management of Police Information MOPI and the Criminal Procedures and Investigations Act 1996; and /or

b) In accordance with the SY/SX's complaints / conduct investigation policies.

c) Examples of where exceptionally this material might be retained for longer could include where a complaint has been made about an officer and so the footage is retained in accordance with the relevant complaints/conduct investigation polices. Alternatively, if the live CCTV feed in addition to performing its role in the LFR deployment also happened to capture evidence of a crime being committed then the video may be retained for the purposes of that criminal investigation and potential prosecution in line with normal operating practice and procedures.

Deployment location privacy considerations. Many deployment locations will be identified as being necessary by the intelligence case supporting the prospects of locating persons at the site and/or how LFR plays a role within wider policing tactics. However, Authorising Officers must also consider the

reasonable expectations of privacy the public may have when traversing a public place where LFR is being considered for deployment. Some places, and the people expected to be at some places by their nature attract greater privacy expectations than others. Authorising Officers also need to consider what measures are appropriate to identify the use of LFR when it is deployed, particularly where expectations of privacy may be greater. This is important to establish if the proposed use for LFR, and the deployment location itself is proportionate.

Authorising Officers should also consider if a proposed deployment location attracts privacy concerns by reference to those expected to be at a particular location, as well as by reference to any specific considerations arising from the context of the location or the positioning of the zone of recognition within it. For example, a deployment in a public space will still need to consider whether the angle of the live feed captures detail beyond that public space such as by viewing into windows of private homes or sensitive locations or over fences into private land.

Footage of a standard commercial high street presents very different considerations to that say of a street with a religious building, or a refuge, a sexual health clinic or other similar potentially sensitive location. Some places, and the people expected to be at those places (by their nature) attract greater privacy expectations than others. It will be necessary to scrutinise whether the precise location of the proposed deployment is suitable and appropriate or whether adjustments are needed to accommodate any specific extra concerns of this nature. For example, this might be where there is only a single entrance to a sensitive location that would fall within the area covered by the LFR system and so individuals may be prevented from accessing (or decide they are unable to access) that building because of the deployment. In such circumstances the Authorising Officer might conclude to slightly adjust the deployment location so that the relevant entrance is outside the scope of the LFR system (unless coverage of that entrance is essential to the purpose of the deployment and the interference this creates to individuals is outweighed by the wider public interests in the deployment).

Measures identifying to the public that LFR processing is taking place must be appropriate and effective at each deployment and so tailoring may be necessary (such as by ensuring signage is lit as needed for deployments where there are low light levels). This will include considerations as to signage and format, in some cases additional languages beyond English may be advisable or required. Similarly, some contexts may need identification to be more than just in written form to be effective where it is likely that at least some of the individuals that will be subject to the LFR will not be adequately made aware of the deployment by written material alone (for example because of reasons of disability or otherwise). Timing should also be considered when assessing proportionality in the context of the location and the purpose of the deployment.

Example: Areas particularly focused on providing facilities or attractions aimed at children would typically attract greater privacy expectations over an area that typically sees attendance from the public more broadly. The public would not typically expect LFR to be sited outside a toy shop or school that may disproportionately see children passing the LFR system if the LFR system could be sited elsewhere. There may nevertheless be instances where the intelligence cases, and the need to protect children makes it necessary and proportionate to deploy LFR to these areas. For example, if it is known that wanted sex offenders are targeting those that visit the location and it not possible to locate them by siting LFR elsewhere or using other less intrusive policing tactics. If it is necessary to use LFR at the location, mitigations to reduce the privacy impact should be used wherever possible. This could include extra measures to ensure that the signage and information about the LFR Deployment is accessible to children who pass through the Zone of Recognition. The signage should be tailored to children where necessary. Consideration should also be given to pre-deployment engagement with the relevant location and those using it (e.g. a briefing to the whole school). Where it is possible to so, and does not increase the risk to children, the time of a

Deployment and configuration of a Zone of Recognition should also seek to minimise the numbers of children assessed by the LFR system.

Areas assessed as having high expectations of privacy which give the public no or little option to avoid the LFR area without substantial inconvenience should generally be avoided unless the following mean that the Authorising Officer is satisfied the use of LFR in the circumstances remains necessary and proportionate:

a) The importance of using LFR in that specific location (rather than any other location) to realise a legitimate aim supports LFR's use.

b) The lack of a viable, less intrusive alternative available for use in the circumstances.

c) Any further mitigations to reduce any impact to the wider public in so far as it is possible to do so., taking account of the legal duties and obligations of SY/SX Police (including but not limited to Equality, Human Rights and Public law). For example, considerable justification would be needed if the only alternative route to avoid the deployment is one that is not wheelchair accessible and mitigations such as a temporary ramp could not be put in place.

d) Considering all the above the level of interference on the public in that location by the context and timing of the LFR deployment is justified and necessary in light of the significant and specific purposes the LFR deployment seeks to serve

Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record the measures taken to ensure the use of LFR causes the least possible interference to the person(s) sought and others. This should include explicit reference to any privacy considerations that may be relevant to a deployment location and any mitigations in place to impact the impact of the LFR deployment. Authorising Officers should then continue to review deployments of LFR to ensure the use case remains appropriate especially as regards any changes of circumstances that will require adjustments to the deployment.

Example: If there was a necessity and proportionality case, based on intelligence, to deploy LFR in a residential suburban area to locate a group of burglary offenders, then there may be a greater expectation of privacy in this area when compared to a non-residential area. To mitigate this, depending on the circumstances it may be necessary to provide additional communication about the use of LFR, for example by leafleting local residents or posting on local neighbourhood social media groups. The timing of the deployment will also need to be considered so that it is timed when it is most likely to fulfil its purpose in locating wanted burglars whilst at the same time minimising how many general members of the public are unnecessarily exposed to the processing (such as for example not operating it during the school-run time window).

3.11 Wider Human Rights Act considerations

The right to privacy is a value which protects the autonomy and human dignity of individuals by enabling them to conduct their lives in a way of their choosing. There are therefore circumstances when freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and of association (Article 11) may be particularly relevant.

a) *Article 9.* The clothing and other items (e.g. jewellery) people wear can be an act of thought, conscience and religion and in normal circumstances, the police do not have the legal power to require a person to remove clothing (including any headdress) simply because they are passing the LFR system. Additionally, the location where people may pass the LFR system may also engaged Article 9 if it may deter or prohibit people accessing a place of worship for example. Given the obligation to justify any such interference as being necessary in each case, consideration will need to be given as to whether changing the timing, location or zone of recognition could deliver on the purposes of the deployment in a way that less infringed this right (e.g. outside of the times of service, or away from the entrance). Alternatively, if those variables can't be changed other considerations such as advance engagement with the effected population so that they can for example make plans to worship elsewhere if they wish to not be subject to LFR.

b) *Articles 10 and 11* have relevance when considering both the policing of assemblies and demonstrations and any use

of LFR which may impact on an assembly or demonstration. Article 10 is especially pertinent should people have reservations about expressing themselves because of an LFR Deployment. Article 11 is also relevant should the use of LFR deter people from attending an assembly or demonstration at all or otherwise cause people to minimise their involvement. Where the purpose of the LFR use, case is inherently tied to the demonstration etc because it is for example looking to identify persons wanted for criminal activities that are assessed as being likely to attend the demonstration. Then it is less likely to be possible to mitigate this infringement by changing the location or scope of the deployment. However, consideration should be given as to whether other measures such as more extensive and prominent publication of the purpose and function of the LFR deployment would help mitigate the risk. Individuals who wish to attend and exercise their Article 10 and 11 rights but for their concerns about being processed by LFR, may not feel inhibited if they are given clear and more extensive than usual information. Including that the deployment will only be to identify persons subject to arrest for previous violent offences who pose a threat to public safety and all those in the demonstration. As well as that the data of all other persons at the demonstration would only be processed momentarily for comparison on a closed automated system before being immediately deleted.

c) *Operational Duties*

The 'operational duty' was first outlined in the case of *Osman v United Kingdom*7 [8] and concerned an alleged failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights in *Osman* found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Caselaw also supports that the police are under an Osman style duty to investigate serious allegations in a timely and efficient manner to uphold an individual's Article 3 rights.

The Osman operational duty has particular relevance to LFR in two contexts (i) being used to locate those posing a threat to the public or themselves where a

[8] [1999] 1 F.L.R. 193 (ECtHR)

real and immediate risk to life is identified and LFR is thought to provide an appropriate response to such risk and (ii) on an Alert being generated where the need to locate that person may engage the Osman operational duty with measures being put in place should a person generating an Alert seek to evade officers.

d) *Article 14.* This right requires that all the rights and freedoms provided for in the Human Rights Act 1998 (and ultimately from the European Convention on Human Rights) must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and have equal access to them. Article 14 is not a stand-alone right – there is a need to show that discrimination has affected the enjoyment of one or more of the other human rights, not that the other rights have been breached. As a result, there are two primary points to consider in relation to the LFR system (i) does the LFR system and operational process perform such that the demographic differential performance varies by a particular demographic which results in a person suffering a discriminatory effect and (ii) if there is a different in treatment, is this capable of an objective and reasonable justification. Further detail on this is set out within the relevant EIA[9], but in summary the LFR system used by SY/SX has undergone testing by the National Physical Laboratory assisting the SY/SX with further understanding on how to use the software fairly and helps to ensure our legal responsibilities under Human Rights and protected characteristics are met as regards the functioning of the electronic system. This document and the wider LFR documents alongside operational practice and standard training help to ensure helps to ensure our legal responsibilities under Human Rights and protected characteristics are met in relation to the wider operational activity necessary as part of a LFR deployment.

[9] Live Facial Recognition | Surrey Police and Live Facial Recognition | Sussex Police

4 Equality Act 2010

4.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination based on different treatment based on a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, SY/SX must comply with section 149 of the Equality Act 2010 which is most known as the Public Sector Equality Duty ("PSED").

4.2 SY/SX is required to take measures to ensure that the use of LFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of the LFR system (as regards whether performance varies by any demographic), and (b) the operational Deployment of the LFR system:

a) The technical performance of the LFR system.

The Court of Appeal Bridges decision makes it clear that the PSED requires SY/SX to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the specific LFR technical system and operational procedure used does not have an unacceptable bias on grounds of race or sex (or any other protected characteristic). To assist the public with understanding how SY/SX meets its PSED duties, SY/SX has published the SY/SX LFR Equality Impact Assessment. Additionally, the specific software and algorithm used by SY/SX has been independently tested by the National Physical Laboratory.

- **Independent evaluation:** Several studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result, regard has been taken 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 NEC – the provider used by SY/SX. This was taken further with the National Physical Laboratory (NPL) who have undertaken a scientifically underpinned evaluation of the LFR algorithm, used by SY/SX, in the operational environment and published their conclusions as regards the LFR algorithm's

performance.[10]

- **Ongoing assurance:** SY/SX LFR Documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and offers SY/SX a chance to monitor for technical or other issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, SY/SX would then explore that further and test for issues under the oversight and scrutiny of the SY/SX Facial Recognition Technology and Biometrics Programme Board.

b) The operational Deployment of the LFR system.

SY/SX LFR Documents are also responsive to how specific subject-related, system-related and environmental factors may influence the LFR system in the circumstances and context where it generated an alert and if such factors combine to mean an engagement with a member of the public is not appropriate in the circumstances. This seeks to ensure the LFR system is suitable for its intended use and operating correctly. Subject, system and environmental factors including aspects such as camera configuration, camera location, lighting conditions, the distance at which people will pass the LFR system, crowd flow levels in so far as this may result in occlusion (including by reference to the height of the subjects being sought) and points relating to an individual's age and appearance have been considered carefully in SY/SX LFR Documents to ensure the efficacy of the LFR system and the SY/SX's compliance with its Equality Act 2010 duties.

By way of example, SY/SX LFR Documents provide that LFR Operators are trained to identify watchlist issues with proposed images which may impact on system performance. Where the need to use an image is deemed to be necessary and proportionate, those using the LFR system have received training to maximise the LFR system's performance and to effectively consider any issues arising from the use of such images as part of the identification process.

Having taken reasonable steps to understand the statistical accuracy and demographic performance of the SY/SX LFR system and then considering points relating to subject, system and environmental factors, and the framework of safeguards implemented, SY/SX has adopted a 'fail-safe' position to ensure

[10] frt-equitability-study_mar2023.pdf

that in the absence of there being other lawful grounds to take policing action:

> **No Engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own opinion that there is a match between the member of the public and the watchlist image.**

This means the LFR system is not making a final decision that there is a actionable match nor does it make any decision on whether to take any further action as a result of that match, an officer makes both of these decisions - just as officers make similar decisions to engage with members of the public every day (without the support of LFR). The officer is best placed to make this decision, drawing on their training and policing experience.

LFR is the catalyst to police activity based on information/intelligence that already exists within our crime and intelligence database Records Management System.

Similarly, the officer is best placed and is required to consider the impact of any subject, system and environmental factors which may have influenced the LFR system when it generated an alert. These factors may combine to mean an engagement with a member of the public is not appropriate in the circumstances. The officer is best placed to make this decision, drawing on their training and policing experience and aware of their legal duties and obligations. For example, this might be where at the end of a deployment when light levels have dropped an alert is generated against a watchlist image. Upon review the officer considers the changed lighting conditions and in comparing the images and concludes it is a false positive because of this environmental factor.

Authorising Officers: To ensure that the officer is best able to make an informed decision on any engagement, all officers who are part of an LFR deployment are to have been briefed on the operation of the LFR system. This includes Subject, System and Environmental Factors that can impact performance. LFR Engagement Officers should also have been given training relating to unconscious bias given their key role in the Engagement decision making process.

Beyond subject, system and environmental factors, SY/SX personnel are also familiar with managing the Public Sector Equality Duty (PSED) requirement whilst undertaking policing activities from several other crime fighting techniques, for example, ‘stop and search’. In this respect, it is important that the use of LFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment and, where relevant, the Community Impact Assessment informs the policing plan to support the Deployment of LFR to mean SY/SX upholds the PSED. Compliance with the Equality Impact Assessment will then be monitored and reviewed for the duration of that Deployment in addition to general overarching reviews that

will take place periodically.

5 Data protection Act 2018

5.1 SY/SX processes personal data for LFR 'based on law'; specifically, its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate, and the policies put in place by SY/SX LFR Documents. The DPIA, the Appropriate Policy Documents and other SY/SX LFR Documents published by the SY/SX as a public body allows the public (including those passing an LFR system and those who may be placed on a Watchlist) to understand the standards SY/SX operates to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

5.2 For the purposes of Law Enforcement processing (such as preventing crime and disorder), Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including sensitive processing, whether processed on a computer, CCTV, still images or other media. Any recorded image or dataset which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR both in terms of processing relating to those on a Watchlist but also in terms of processing biometric and image information of members of the public to confirm they are not a match to anyone on a Watchlist. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

> *"For the purposes of this Part, "the law enforcement purposes" are 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."*

Authorising Officers: Authorising Officers already need be satisfied of the necessity to use LFR to prevent crime and disorder and ensure public safety in the context of the Human Rights Act 1998. Similarly, to satisfy Section 35(5) DPA, they need to be content that the LFR system's processing of biometric data is strictly necessary for the law enforcement purpose. The law enforcement purpose should be clearly identified and the way in which the strictly necessary standard has been met explained in each case. Any deployment can seek to serve multiple purposes, and so a deployment watchlist may be a composite of several purpose specific watchlists providing there is proper compliance for all of them (including any purposes relating to UK GDPR rather than Part 3 processing)

a) Strictly necessary in this context means that the processing

must be more than merely necessary, it must be such that this processing is required to give effect to the relevant purpose, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via LFR is not used in a manner that is contrary to the identified purpose or in any way that does not meet the high bar of 'strict necessity'

Example: alternative policing methods to prevent threats to public security: LFR may be deployed to police a high profile well-attended public event. When considering alternatives, in this example, other measures such as extra CCTV may be considered. However, they will not always be a viable less intrusive alternative in the circumstances. For example:

1. Whilst CCTV can help ensure event safety, it lacks the ability to proactively Alert officers to the potential presence of individuals of interest to them.
2. It may not be practical to expect officers to recognise larger numbers of people of interest to the Police given the nature and scale of the event, the numbers of officers available to police the event and the flow rate and number of people passing the CCTV system. This is especially relevant where the importance of making such identifications supports the use of a more suitable alternative such as LFR. This may also mean that use of LFR is more proportionate and privacy protecting given LFR works on a secure and closed system that would not require the disclosure of personal data to large numbers of officers as would be the case if more traditional location tactics were deployed instead.
3. Where LFR is thought to offer further important protection to the public as opposed to other policing methods. For example, this may apply where the law enforcement purposes for a Deployment include wider public safety considerations. These may include the need to locate those wanted by the courts. Such persons may attend such a high-profile event and, in line with the decision of the courts to require their arrest, pose a risk to the public generally. Alternatively, where there is concern that persons might attend an event to cause disruption or carry out criminal acts the deployment of LFR system and signage may significantly contribute to the prevention of such crime and the protection of the public attending by acting as a deterrent effect convincing those persons intending to cause trouble to not attend given the presence of LFR.

b) In assessing whether the 'strictly necessary' standard has been met, the Authorising Officer must consider all relevant factors including:

- What other policing methods have been used / discounted when seeking to locate an individual(s) on the watchlist or to provide a series of tailored security measures.
- The importance of achieving the specific relevant purpose(s) of the deployment and the prospects of achieving those purposes through the deployment of LFR at the proposed location with the proposed watchlist

(for example, is the deployment intelligence-led or otherwise supported by information which confirms that LFR can be expected to get results in the circumstances being contemplated).

- The size and scale of the planned LFR deployment and associated watchlist and the level of sensitive/special category processing anticipated because of the LFR Deployment (both in terms of watchlist and life feed processing)
- If the relevant purpose which underpins the use of LFR is strictly necessary and proportionate to the need to undertake sensitive/special category processing and the risk to individuals' rights this entails (subject to all the overarching and deployment specific protections and safeguards implemented).

Schedule 8 conditions of the DPIA[11] are engaged, the most likely to be applicable are:

a) necessary for the exercise of a function conferred by an enactment or rule of law – for reasons of substantial public interest.

b) necessary for the administration of justice.

c) necessary to protect the vital interests of the data subject or another individual.

d) necessary for the safeguarding of children and of individuals at risk.

e) necessary for the purpose of preventing fraud.

Example: The use of LFR will assist SY/SX in fighting knife crime in support of its common law policing powers. LFR could be deployed to identify wanted offenders who have failed to comply with court bail relating to such offences. Used in this way, LFR would assist in the prevention, investigation, detection or prosecution of criminal offences and be both necessary for the administration of justice as well as necessary for the exercise of the functions conferred on the police under both statute and the common law

LFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description to scan a crowd and try and spot an offender where positive results would otherwise be less likely and the risk of people being missed, higher. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context LFR's use may be seen as strictly necessary to support the investigation of knife crime, to enable the SY/SX to effectively respond to a pressing social need.

For similar reasons, the court in the *Bridges* cases accepted the substantial public interest in the

[11] Live Facial Recognition | Surrey Police and Live Facial Recognition | Sussex Police

police using LFR to discharge their common law policing duties.

5.3 Test SY/SX has also undertaken several steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the LFR system. Actions are set out in the remainder of this section.

5.4 Data Protection Impact Assessment:

DPIA has been conducted to support the use of LFR to identify and minimise the data protection risks. Whilst the LFR DPIA will be under constant review, consideration will be given as to whether any changes are needed following each deployment, and a comprehensive review will be conducted on at least an annual basis. Authorising Officers authorising the use of LFR are required to ensure there is a DPIA in place which is sufficient for each Deployment. Specifically, consideration should be given to:

a) if the risks and controls remain current and sufficient for the specific planned use of LFR in the proposed deployment; and

b) if the planned use for LFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.

5.5 Data Protection by Design:

Several data protection controls have been designed into the LFR system and procedure to mitigate processing impacts on privacy and to comply with the general obligation in appropriate technical and organisational measures having considered and integrated data protection compliance into all aspects of LFR processing activities. The designed-in measures identified in the DPIA[12] of this document, include measures to:

a) limit the amount of personal data collected, ensuring the application of the principle of data minimisation at all stages but as to what is included in a watchlist and as regards what is processed from the live feed.

b) limit the extent of personal data processing to that which meets the necessary requirements and goes no further.

c) limit the period of personal data storage by carefully considering and keeping under review both the overarching retention schedule but also whether in any case the information could cease to be processed at an earlier point.

In implementing a privacy by design approach, the LFR system has been constructed with several physical and technical security measures including:

a) A condition that requires that watchlist images are transferred onto the LFR system via a USB using an AES-CBC 256-bit full disk hardware encryption engine, that is further protected by a

[12] Live Facial Recognition | Surrey Police and Live Facial Recognition | Sussex Police

passcode.

b) The LFR system is a fully closed system (isolated from both internet and force network), with two layers of password protection to access the application. The LFR system is physically protected when in use and securely wiped following each deployment.

c) Role based access controls with limited user permissions are implemented on the LFR system, including logins by trained operators.

d) The Dashboard and RESTful API are secured with SSL and TLS by default.

e) All connections are directed through HTTPS within a closed system.

f) A full audit is maintained of all users-initiated actions undertaken during a deployment.

g) Technical issues with the LFR system are always dealt with by the specific member of the technical staff who supports the Deployment of the LFR system.

5.6 Appropriate Policy Document:

The DPA requires that in relevant circumstances such as the LFR processing of sensitive / special category data, that to be compliant at the time that the processing is carried out, the controller must have an appropriate policy document in place. SY/SX has produced these documents and published them. They allow the public to understand in relation to both law enforcement and UK GDPR processing the details of the:

a) the data being processed by the LFR system, how often it is processed and whose data is processed.

b) procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition to process biometric personal data both for those on the Watchlist and those passing an LFR system.

c) SY/SX policy for the retention and erasure of personal data for LFR processing.

5.7 Data Protection Officer:

SY/SX has appointed a Data Protection Officer (DPO) each per force in compliance with the DPA. Each of whom have been consulted in relation to LFR. The DPOs are available to inform and advise the Chief Constables (as data controller) and SY/SX personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

6 General Data Protection Regulation (GDPR)

6.1 As part of SY/SX' common law powers to protect and preserve life and property, we process special category data in accordance with the requirements of Article 9 of the UK GDPR (which is incorporated into UK law under and supplemented by Part 2 and Schedule 1 of the DPIA).

6.2 The Schedule 1 DPA conditions for processing special category data require SY/SX to have an DPIA in place, setting out and explaining our 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.

7 Protection of Freedom Act 2000

The Protection of Freedoms Act 2012 (PoFA) saw the introduction of a new surveillance camera code issued by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. Section 33(1) PoFA requires SY/SX to have regard to the Code for the use of LFR. This includes compliance with the 12 guiding principles that system operators should adopt. The Code makes several specific points in relation to automated recognition technologies which SY/SX have regard to as follows:

Code	SY/SX approach
Fair processing information to data subjects	SY/SX processing information publicly available to data subjects. It makes information relating to the LFR and data processing available via its website. The LFR deployments are publicly disclosed with supporting information.
Appropriate retention and disposal systems	The necessary systems are addressed in the SY/SX LFR documents.
Suitable technological and physical security measures	These measures have been addressed by design and are also covered in the SY/SX LFR documents.
Cameras of sufficient quality to meet the intended purpose	This requirement is addressed by the design of the LFR system and is covered in the LFR documents.
Monitored by trained individuals	The LFR system will always flag possible matches to a trained member of SY/SX personnel for a decision on any further action. In this way, the LFR system works to assist SY/SX personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

8 Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

a) public authorities are obliged to publish certain information about their activities.

b) members of the public are entitled to request information from public authorities.

In recognition of their FOIA duties, SY/SX makes significant LFR information available via its website. This includes both framework documents such as the APDs and summary information relating to LFR deployments including the watchlist size, the total number of Alerts, positive action and incorrect identification numbers, arrests and disposal numbers and estimates of the total number of faces seen as people passed the LFR system. SY/SX will also be responsive to FOIA requests.

9 Legal Framework and Governance Overview

Pictorial summary of existing legislation and related governance regards policing's overt use of Live Facial Recognition