North Wales Police Live Facial Recognition (LFR): Legal Mandate

Summary: Outlines the legal basis for North Wales Police's use of LFR technology

Name of Force	North Wales Police (NWP)
Subject	Live Facial Recognition (LFR)
Summary	Outlines the legal basis for NWP's use of overt LFR technology to locate persons on a Watchlist
Author	Sergeant Joseph Dunn

Project Name	Live Facial Recognition Technology
Senior Responsible Office-	ACC Chris Allsop
Business Area/Department	Operational Support Services
Proposed implementation date	Immediately

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	23.04.24	Project manager	Sergeant Joseph Dunn	Initial Draft
0.2	26.04.24	Legal Services	Karen Kinsey	Legal Review – minor amendments
1.0		SRO	ACC Chris Allsop	

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

1 Introduction

1.1 At the time of writing, LFR for law enforcement purposes is not subject to dedicated primary legislation. LFR is 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.

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 d) Data Protection Act 2018 (Part 3) e) UK General Data Protection Regulation f) Protection of Freedoms Act 2012 g) Police and Criminal Evidence Act Code D
	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) Secretary of State's Surveillance Camera Code of Practice. b) Guidance issued by the Surveillance Camera Commissioner (Facing the Camara) c) Information Commissioner's Office Code of Practice for Surveillance Cameras and associated guidance issued by the Information Commissioner
Tier Three: NWP LFR Documents	Regulating the use of LFR	a) NWP Policy Document b) NWP Standard Operating Procedures c) NWP Data Protection Appropriate Policy Document

		d) NWP's Data Protection Impact Assessment e) Equality Impact Assessment Screening Tool f) Community Impact Assessment g) NWP Legal Mandate

2 Common Law

2.1 The police have a number of long-established policing responsibilities and powers derived from common law which have been recognised by the courts. NWP is obliged to comply with common law and statutory safeguards in delivering its policing operational duties and relies on common law to discharge a number of its duties.

2.2 Key common law powers that NWP 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: NWP uses 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 NWP to discharge its responsibilities to protect life and property. It would also be compatible with NWP's duty to bring offenders to justice by facilitating a prompt and effective investigation.

2.3 The use of NWP'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".

Authorising Officers: When considering the use of LFR technology, you must be clear as to the common law policing power that is relied upon for lawfully authorising the use of LFR and record this as part of the decision-making process.

3 Police and Criminal Evidence Act 1984

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

3.2 Allows for the photographs to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

4 Human Rights Act 1998

4.1 NWP's use of LFR must comply with 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. 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 demographic 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.'

4.2 As a qualified right, any interference with an individual's Article 8 rights 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 seeks to achieve the **legitimate aim**;

c) it 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.

4.3 It is well-established that the reach of Article 8 can be broad. The case of *S 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]

4.4 The *Bridges* cases in the High Court and Court of Appeal 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 then 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

[1] *(2009) 48 EHRR 50, at [66 and 67]*
[2] *At [104]*

expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. Authorising Officers should contact the NWP Legal Team should they consider a proposed deployment may have a wider human rights point to consider.

4.5 **There is a legal basis for the interference with the qualified right that the public can understand**

LFR will be used to allow NWP to discharge its well established operational duties pursuant to common law. The courts have recognised that "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 applicants could have their personal information noted down and retained by the police as they occupied publicly accessible space. The court recognised the police's common law powers to 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 will include photographs lawfully held by police, taken in a custody environment, and in line with PACE code D. Any photographs used by police must be current and accurate.

The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect's accomplice or of anyone else. The court confirmed the "key 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]

If photographs are provided to the police for use, such as in cases of a high risk or medium risk missing person, then consent needs to be recorded from the family / person providing the photograph. Details around the usage of photographs and the compilation of the watchlist can be found in NWP's Policy and Standard Operating Procedure for LFR.

4.6 In the case of NWP's use of LFR, this 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]:

[3] R (*Catt) v Association of Chief Police Officers [2015] A.C. 1065* at [11].
[4] Per Laws J in *Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804 at 810F*
[5] *At [69].*

"the legal framework which regulates the deployment … does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined."

4.7 The Court of Appeal Bridges decision further noted that, to be 'in accordance with the law' the legal basis must:

"be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself".

4.8 The *Bridges* case related to South Wales Police's use of LFR. In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held to determine *where* they deployed facial recognition technology and *who* they deployed it to locate those on a Watchlist. The court refers to this as the "Who Question" and the "Where Question". These questions are addressed in the following paragraphs.

The 'Who' Question: When considering how the 'Who Question' should be answered, the Court of Appeal made it clear that the law does not seek specific confirmation as to who is on a Watchlist (they recognise the Neither Confirm nor Deny principle[6]). The Court of Appeal recognised that individuals could be added to a Watchlist on the basis that they are wanted on suspicion of an offence, wanted on warrant and vulnerable persons.

The Court of Appeal also explains why a category of those "other persons where intelligence is required" was not accessible and foreseeable to 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" – essentially 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. NWP addresses this through the provisions under Section 5 of our Standard Operating Procedure, which sets out clear criteria for watchlist inclusion, and the officer applying to the Authorising Officer (ACC Rank) must set out the proposed watchlist and the intelligence based rationale for it. To ensure compliance with the Standard Operating Procedure, the application form sent to the Authorising Officer, and the Record of Authorisation made by that officer must confirm that the deployment adheres to the principles within it around watchlist generation and compilation.

NWP sets the criteria that applies to govern the images that may be included on a Watchlist and in what circumstances. To ensure the criteria is clear, precise, accessible and foreseeable, NWP explains within the Standard Operating Procedure 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.

The 'Where Question: The Court of Appeal noted that the South Wales Police team "was not able to draw to our attention anything which specifies where AFR Locate may be deployed". To ensure

[6] *At [95].*

that this will not be the case with any NWP deployments, our Standard Operating Procedure answers this question within section three. In line with College of Policing APP, any deployment location proposed must be based on reasonable grounds to suspect that the deployment location is one where a person on the watchlist will attend at a time, or at times, when they are sought by means of LFR. Therefore, there must be documented rationale that the location is suitable for deployment based on these reasonable grounds for suspicion. 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, supressing crime hotspots, and getting ahead of crime trends).

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 NWP's Policy and Standard Operating Procedure to support the use of LFR allows the principles contained within this LFR Legal Framework 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 NWP 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.

4.9 **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 in the context of assisting NWP to locate offenders will help NWP achieve its law enforcement purposes.

The means by which NWP may use LFR will be an operational decision within the parameters of the law and the NWP 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.

FAO Authorising Officers: At the point that it is decided to deploy LFR, the decision maker must be clear as to its purpose and how using LFR will help NWP 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 Rights.

4.10 **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 NWP combat crime in areas where LFR has the greatest potential to assist. It is a tool that helps NWP to discharge its operational responsibilities, primarily to help prevent and detect crime and protect the most vulnerable.

FAO 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. 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 NWP to achieve its legitimate aim. In deciding the use of LFR to be necessary, the AO must articulate the issue which LFR was intending to address and how LFR would be deployed to address that problem.

Additionally, in a climate where police forces need to operate efficiently, NWP is cognisant that technology such as LFR can assist with the challenges of quickly and cost efficiently 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 in the area of the Deployment.**

The intrusion to those passing the system is no greater, but (i) the potential to protect the public from those wanted by the courts, (ii) the results from deployments where those with outstanding warrants were included and (iii) the resultant arrests justified the inclusion of those with outstanding warrants from the courts as a *necessary* action to bring offenders to justice.

4.11 **The use of LFR is proportionate to 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:

1) The use of LFR should be a reasonable use of NWP 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 give consideration to the composition of the Watchlist compiled for the LFR system to match against, to ensure that it is not compiled in an excessive 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.

With this is mind, the Watchlist compiled for each deployment of LFR should be current; based on those currently of interest to NWP and/or wider UK law enforcement to mitigate the risk of

the LFR system matching with those no longer of interest to NWP and/or wider UK law enforcement.

2) Consideration should be given 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 NWP 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.

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 NWP. It can also be used for a limited period, targeted, based on wider intelligence, and at 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 NWP 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.

FAO 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 NWP's aim.

3) 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. LFR will be used for a limited time – with a limited footprint, with a defined purpose (controlled by way of the NWP 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 NWP LFR Documents also provides a structure for awareness measures which respond to the nature and objectives of the use of LFR.

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

I. LFR cannot be used to locate persons unless they have been included on a Watchlist.
II. The creation of any Watchlist is specific to the deployment of LFR and is 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.
III. Images on a Watchlist will be lawfully held by NWP with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Watchlist.
IV. Authorising Officers need to expressly consider and approve the use of non-police originated images on any Watchlist. This is because particular privacy considerations may attach to an image where it originates from outside of a policing 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. In specific regard to non-police originated images, even when NWP can lawfully hold the images, the need for the Watchlist to be a proportionate policing response to achieve a lawful policing objective requires the Authorising Officer to undertake a careful assessment of an individual's privacy expectations against the policing need to locate them using LFR. The Authorising Officer's authority must set out their considerations of a balance between the rights of the individual and the interests of the community, taking into account the actual aim of an operation, it's anticipated benefits, and the impact upon the individuals whose biometric data is processed. The NWP LFR Standard Operating Procedure outlines considerations regarding non-police originated images for Authorising Officers at Section 5.
V. On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow police personnel to consider and manage the risk of poor-quality images generating inaccurate LFR Alerts.
VI. All Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment.
VII. The cameras used in the LFR system are of sufficient quality for the LFR system's needs.
VIII. The LFR system is 'closed' and not connected to other NWP or SWP systems or the internet.
IX. The LFR system is designed to assist NWP personnel locate people. The LFR system will always flag potential matches to at least one officer for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.
X. 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:

1. where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*
2. 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.

3. watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.
4. where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 24 hours following the conclusion of the deployment.

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

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or

2. in accordance with the NWP's complaints / conduct investigation policies.

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 general public may have as a whole 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.

Authorising Officers should also consider if a proposed Deployment location attracts particular privacy concerns by reference to those expected to be at a particular location.

> **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 case, 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. 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 little option to avoid the LFR area without substantial inconvenience should generally be avoided unless the Authorising Officer has considered the below principles, and is still satisfied that the use of LFR in the circumstances remains necessary and proportionate:

1. the importance of using LFR in that location to realise a legitimate aim supports LFR's use;

2. the lack of a viable, less intrusive alternative available for use in the circumstances; *and*
3. any further mitigations can be implemented to reduce any impact to the wider public in so far as it is possible to do so.

> **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 we understand 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 we may provide additional communication about the use of LFR, for example by leafleting local residents or posting on local neighbourhood social media groups.

> **FAO 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 particular 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.

4.12 **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.

1. Article 9. The clothing 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 engage Article 9.

> **Example**: The use of LFR can assist NWP to ensure public safety, including at a place of worship where the intelligence case has identified a threat to the public. A decision to place a LFR deployment outside a place of worship or in a way that substantially impedes access to a place of worship can engage Article 9.
>
> In this context, the public safety considerations need to be balanced against the need to use LFR at that location. If the public safety policing objectives could be achieved by deploying the LFR system elsewhere, it would not be necessary to deploy LFR at the proposed location.
>
> If the threat makes it necessary to site LFR near to a place of worship, Authorising Officers also need to determine if the infringement on Article 9 rights is disproportionate to the likely benefits of using LFR. Considerations would typically include the impact on those seeking to access a place of worship, the likely impact on the same people without LFR (being potentially impacted by other policing measures or site closures) and the benefits to safety that LFR brings to the public.

2. Article 10 and 11 have particular 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 as a result 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.

> **Example**: The use of LFR can assist NWP in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. In deciding whether the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting that there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of the LFR deployment.
>
> Article 10 and 11 rights must be balanced against the need to use LFR to enable an assembly that might otherwise be disrupted by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of LFR. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety. They could also include there being focus placed on ensuring the public understand the use of LFR is to help them safety undertake their assembly.

3. Operational Duties

The 'operational duty' was first outlined in the case of *Osman v United Kingdom*[7] 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. Case law 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 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.

4. Article 14. This right requires that all of the rights and freedoms set out in the Human Rights Act 1998 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 actually breached. The use of LFR will be relevant in circumstances where demographic performance of the

[7] [1999] 1 F.L.R. 193 (ECtHR)

LFR algorithm varied to such an extent that people of a particular demographic were more or less likely to see a False Alert generated against them. As a result there are two points to consider in relation to the LFR system (i) does the LFR system's demographic differential performance vary by a particular demographic such as it results in a person suffering a discriminatory effect and (ii) if there is a different in treatment, is this capable or an objective and reasonable justification. As is demonstrated within Section 12 of NWP's LFR Policy, NWP is confident that the use of LFR in its current format on mutual aid from South Wales Police does not demonstrate any discrimination.

5 Equality Act 2010

5.1 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 on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, NWP must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty ("PSED").

5.2 NWP 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 (and then, if performance varies by any particular demographic), and (b) the operational Deployment of the LFR system.

Each will be addressed in turn:

1. The technical performance of the LFR system.

The Court of Appeal *Bridges* decision makes it clear that the PSED requires the police to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias on grounds of race or sex.

North Wales Police uses LFR technology supplied and operated by South Wales Police, and we are confident in the work undertaken by SWP to comply with their PSED duties. As the *Bridges* case related to South Wales Police, to assist the public with understanding how they meets their PSED duties, SWP has published the SWP LFR Equality Impact Assessment which is available on their website through the following link: frt-eia--v1.4-sl.pdf (south-wales.police.uk).

Additionally, the following steps have been taken to understand the statistical accuracy and demographic performance of the LFR algorithm. This includes:

1. Independent evaluation: A number of 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 SWP has paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by SWP. SWP has then taken this further with the National Physical Laboratory (NPL) who have undertaken a scientifically underpinned evaluation of the SWP's LFR algorithm in the operational environment and published their conclusions as regards the SWP LFR algorithm's performance. North Wales Police has then reflected the findings of this in our LFR Policy and Standard Operating Procedure to inform our operational practice.

2. Ongoing assurance: The NWP LFR Documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and also offers NWP a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, NWP, in conjunction with SWP would then be in a position to explore that further and test for issues under the oversight and scrutiny of the SWP Facial Recognition Technology and Biometrics Programme Board, and the NWP A.I Ethics Board.

3. Independent academic evaluation:

In August 2021 South Wales Police was awarded Home Office Science, Technology, Analysis & Research (STAR) funding to undertake testing of the accuracy and equitability of FRT in an operational environment for LFR, OIFR and RFR.

In collaboration with the Metropolitan Police (MPS), this work was awarded to the National Physical Laboratory (NPL) at the end of 2021. The NPL is a prestigious world-leading centre of excellence that provides cutting-edge measurement science, engineering and technology to underpin prosperity and quality of life in the UK. In order to deliver on the objectives of the research, it was necessary to use and document the use of LFR in an operational setting within UK policing. Data collection for the evaluation took place in July and August of 2022 alongside five operational deployments of LFR, four in London and one in Cardiff.

A cohort of volunteers were selected to take part in the study who were of varying age, gender and race, the volunteers were seeded into the crowd passing the LFR System at each deployment so as to appear in the LFR video footage.

The data was then evaluated 'post event' with a balanced Watchlist and facial photographs taken of the volunteers in a variety of settings to realistically replicate the use cases for LFR, RFR and OIFR.

The full results are presented in the National Physical Laboratory's commissioned report 'Facial Recognition Technology in Law Enforcement Equitability Study'.

The NPL report gives us an impartial, scientifically underpinned, evidence-based robust analysis of the performance of the LFR FRT System used by NWP in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.

In summarising LFR operational performance, NPL have provided performance figures for two different Watchlist sizes: (i) a Watchlist of 10,000 reference images, which is broadly in line with those used on the MPS' LFR operational deployments to date and (ii) a watchlist of 1000 reference images a size more typical for SWP LFR deployments (examples of MPS and SWP figures are given, as these are the two forces in England and Wales who host LFR capability).

The performance figures use industry standard measures; (i) True-Positive Identification Rate (TPIR) (also known as True Recognition Rate)– the rate of successful recognition when subjects on the Watchlist pass through the Zone of Recognition (ii) False-Positive Identification Rate (FPIR) (also known as False Alert Rate) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the Watchlist pass through the Zone of Recognition

In relation to LFR, NPL found that at a Threshold of 0.60, any differences in TPIR by gender, by race, or by race/gender combined were not statistically significant. **This means that the systems performance is not biased towards any race or gender.**

The study has shown that at Thresholds of 0.60, 0.62 and 0.64 the number of subjects with a false positive is very small and there is no statistically significant imbalance between demographics.

1.1 The study has shown that at a face match Threshold of 0.64 or higher the probability of false positives being created at a setting of 0.64 are less than 0.001% or 1 in 60,000.
Thus, at this Threshold the FPIR is identical for race, age and gender. **North Wales Police only deploy LFR at a Threshold setting of 0.64.**

4. The operational Deployment of the LFR system.

NWP LFR documents are also responsive to the Subject, System and Environmental Factors 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 the NWP LFR documents to ensure the efficacy of the LFR system and therefore NWP's compliance with its Equality Act 2010 duties.

By way of example, NWP 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.

As a result of having taken reasonable steps to understand the statistical accuracy and demographic performance of the NWP LFR system and then in light of points relating to Subject, System and Environmental Factors, and the framework of safeguards implemented as a result, NWP has adopted a 'fail-safe' position to ensure that no engagement will occur with a member of the public unless at least one officer has reviewed an LFR system generated potential match and reached their own opinion that there is a match between the member of the public and the Watchlist image.

This means that the LFR system is not making any decision to engage with the public, the officer is making this decision - 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.

Similarly, the officer is best placed to consider the impact of any Subject, System and Environmental Factors which may have influenced the LFR system when 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.

FAO Authorising Officers: In order 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. This briefing and training will be provided by the dedicated SWP lead deployed as part of the Mutual Aid capability.

Beyond Subject, System and Environmental factors, NWP personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of 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 which is completed prior to any deployment informs the policing plan to support the deployment of LFR to mean that NWP upholds the Public Sector Equality Duty.

Compliance with the Equality Impact Assessment will then be monitored and reviewed for the duration of that deployment.

6 Data Protection Act 2018

6.1 NWP 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 the NWP LFR Policy and Standard Operating Procedure. The Appropriate Policy Document, Data Protection Impact Assessment and the Policy and Standard Operating Procedure published by NWP as a public body allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards that NWP 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.

6.2 For the purposes of 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 from a device which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR both in terms of locating those on a Watchlist but also in terms of processing biometric information of members of the public to confirm they are not 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."*

FAO Authorising Officers: Authorising Officers already need to 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.

Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means, and that any personal data collected via LFR is not used in a manner that is contrary to the identified law enforcement purpose.

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. 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 actively 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.

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.

The 'strictly necessary' standard may be informed by the Authorising Officer considering factors including:

1. 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;

2. The importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose 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);

3. the size and scale of the planned LFR deployment and associated Watchlist and the level of sensitive processing anticipated as a result of the LFR deployment; *and*

4. if the law enforcement purpose which underpins the use of LFR is strictly necessary and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

FAO Authorising Officers: Authorising Officers need to be satisfied that the processing satisfies one of the Schedule 8 conditions set out below and complies with the six data protection principles.

6.3 Schedule 8 conditions of the DPA:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk; **and**
- necessary for the purpose of preventing fraud.

Example: The use of LFR will assist NWP 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.

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 NWP to effectively respond to a pressing social need.

Similarly, the Schedule 8 condition of being necessary for judicial and statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection, or prosecution of offences to keep the public safe. For similar reasons, the court in the *Bridges* cases accepted the substantial public interest in the police using LFR to discharge their common law policing duties.

6.4 NWP has also undertaken a number of 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. Particular actions are set out in the remainder of this section.

6.5 Data Protection Impact Assessment:

A DPIA has been conducted to support the use of LFR in order to identify and minimise the data protection risks. Whilst the LFR DPIA will be under constant review and no later than on an annual basis, Authorising Officers authorising the use of LFR should ensure there is a DPIA in place which is sufficient for each deployment. Specifically, consideration should to be given to:

a. if the risks and controls remain current and sufficient for the planned use of LFR; and
b. if the planned use for LFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.
c. the Article 8 rights of those engaged by the LFR technology who have their biometric data captured to ensure that the impact considers the other rights that are likely in the assessment of the impact on the individual, or measures taken accordingly.

6.6 *Data Protection by Design*:

A number of data protection controls have been designed into the LFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into LFR processing activities. The designed-in measures identified at paragraph 4.11 of this document, include measures to:

a. limit the amount of personal data collected;
b. limit the extent of personal data processing;
c. limit the period of personal data storage.

Additionally, NWP has acted to ensure that the LFR system performs to a level where the statistical accuracy of the data being processed and fairness 'by design' is ingrained into NWP's LFR system. NWP LFR Documents and other published supporting information explain how NWP is assured that its LFR system operates with a high degree of statistical accuracy and in a way that does not lead to unjust results between demographics.

Further consideration has been given to limiting access to any personal data retained for the 31 day period. The LFR system also includes a number of physical and technical security measures including:

a. 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 pass-number access;
b. The LFR system is a fully closed system 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;
d. The LFR application is connected to mobile devices using a private access point with three levels of protection (i) specific IP addressing, (ii) password access to the access point, and (iii) password access to the mobile app. The mobile app has a RESTful API and will be covered by SSL;
e. The Dashboard and RESTful API are secured with SSL and TLS by default;
f. All connections are directed through HTTPS within a closed system;
g. A full audit is maintained of all user initiated actions undertaken during the course of a deployment; *and*
h. Technical issues with the LFR system are always dealt with by member of the technical staff who support the deployment of the LFR system.

6.7 Appropriate Policy Document:

Section 42 of the DPA requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. NWP has produced this DPIA document. This document allows the public to understand details of:

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 from Schedule 8 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
c. NWP policy for the retention and erasure of personal data for LFR processing.

6.8 Data Protection Officer:

NWP has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to LFR. The DPO is available to inform and advise the Chief Constable (as data controller) and NWP personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

7 General Data Protection Regulation

7.1 As part of NWP's 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 DPA).

7.2 The Schedule 1 DPA conditions for processing special category data requires NWP to have an APD 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.

7.3 Article 9 conditions of UK GDPR are engaged:

- explicit consent and
- substantial public interest

7.4 Section 10 DPA supplements Article 9 GDPR, requiring the following conditions of Schedule 1 to be satisfied (historical research part 1 of schedule 1 / substantial public interest part 2 of schedule 1).

7.5 Schedule 1 DPA (part 1) are engaged:

- statutory etc and research government purposes; and
- safeguarding of children or individuals of risk

7.6 Schedule 1 DPA (part 2) are engaged:

- statutory and government purposes;

- safeguarding of children

7.7 Appropriate Policy Document:

Schedule 1 DPA conditions for processing special category data require NWP to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 GDPR. NWP has produced this document. This document allows the public to understand details of:

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 from Article 9 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
c. NWP policy for the retention and erasure of personal data for LFR processing.

8 Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen 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 NWP 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 a number of specific points in relation to automated recognition technologies which NWP have regard to as follows:

Code	SWP approach
Fair processing information to data subjects	SWP 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, such as signage and leaflets handed to those present at the Zone of Recognition.
Appropriate retention and disposal systems	The necessary systems are addressed within NWP's LFR documents.
Suitable technological and physical security measures	These measures have been addressed by design and are also covered in Section 10 of the NWP LFR Standard Operating Procedure, as well as in section 6.6 of this document.
Cameras are of sufficient quality to meet the intended purpose	This requirement is addressed by the design of the LFR system, and detailed within Section 14 of the NWP LFR Policy.
Monitored by trained individuals	The LFR system will always flag possible matches to a trained member of police personnel for a decision on any further action. In this way, the LFR system works to assist NWP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

9 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:

9.1.1 public authorities are obliged to publish certain information about their activities;

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

In recognition of its FOIA duties, NWP makes significant LFR information available via its website.

This includes 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. NWP will also be responsive to FOIA requests.

10 Legal Framework and Governance Overview – summary of existing legislation and related governance regards policing's overt use of Live Facial Recognition Technology