Data Protection Impact Assessment (DPIA)

You are advised to refer to the guidance material before completing the form.

Data Protection Impact Assessment (DPIA)	
Project Proposal Name:	Live Facial Recognition (LFR)
Force:	Norfolk Constabulary / Suffolk Constabulary
Department/Area:	Norfolk Community Safety department Suffolk County Partnership & Prevention Hub
Force SPOC:	Norfolk – Insp Toby Gosden Suffolk – Sgt Dom Mason
Information Asset Owner:	Chief Supt Mears
DPIA Advisor:	Beth Mortimer
Date approved and signed off by Information Asset Owner:	DD/MM/YYYY
Date on which processing will commence:	22/02/2025
Date submitted to Information Compliance:	27/02/2026
Review	This DPIA will be reviewed following the first deployments in Norfolk. The DPIA should be considered for review before deployment to ensure it is still accurate and reflective of practices.
Version History	V1 – Suffolk Only Pilot V2 – Re-work of template following Joint use of LFR across Norfolk and Suffolk.
Note: DPIA Advisor will endeavour to give an **initial response** within 10 working days of receiving the completed form.	

Information Compliance use only	
DPIA is not mandatory.	☐
DPIA is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	☐
DPIA is mandatory.	☒

Section 1 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

Ensure to avoid technical language and acronyms.

1.0 Please give details of the project/process/system.

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined Watchlist in order to locate Persons of Interest by generating an Alert when a Possible Match is found.

LFR can be a valuable policing tool that helps police forces keep the public safe and to meet their common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

The following are illustrative examples where LFR may assist Forces achieve their policing purposes:

- supporting the location and arrest of people wanted for criminal offences
- preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders)
- supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g., stalkers, terrorists, missing persons deemed at increased risk, etc)

The technical operation of LFR comprises of the following six stages:

1. **Compiling/using existing database of images:** the LFR application requires a Watchlist of reference images against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the 'facial features' associated with their subjects are extracted and expressed as numerical values (a Biometric Template).

   Norfolk and Suffolk Constabulary LFR Policy outlines considerations relevant to lawfully compiling a Watchlist including determining which persons may be on a Watchlist and the sources of Watchlist imagery.

2. **Facial image acquisition:** a CCTV camera takes digital pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition and using it as a live feed. The siting of the CCTV cameras, and therefore the LFR Deployment location is important to the lawful use of LFR. Norfolk and Suffolk Constabulary LFR Policy and SOPS provide considerations relevant to the locations Norfolk and Suffolk Constabulary may select to deploy the cameras when using them for LFR.

3. **Face detection:** Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

4. **Feature extraction:** Taking the detected face the software automatically extracts facial features from the image, creating the Biometric Template.
5. **Face comparison:** The LFR software compares the Biometric Template with those held on the Watchlist.

6. **Matching:** When the facial features from two images are compared the LFR application generates a Similarity Score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A Threshold value is set to determine when the LFR software will generate an Alert to indicate that a Possible Match has occurred. Trained members of police personnel will review the Alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

Relationship to individuals: LFR relates to individuals in three ways:
1) Those on an LFR Watchlist
2) Those passing the LFR system
3) Protecting the public more generally.

Watchlist: The watchlist is bespoke for evert deployment (created within 24 hours of deployment) and the rational for the make-up of the watchlist must be intelligence-led, justified, proportionate and necessary, with the nature of the watchlist recorded prior to each deployment.

The candidate images and related biometric template are deleted immediately post deployment and in any case within 24 hours.

The criteria for constructs of watchlists for use with LFR must be approved by the Authorising Officer and be specific to an operation or to defined policing objective. Watchlist, and any images for inclusion on a watchlist, must also be limited to the categories of image articulated in Norfolk and Suffolk LFR policy documents which are images of people who are:

- Wanted by the courts; and/or
- Suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
- Subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the deployment; and/or
- Missing persons deemed at an increased risk; and/or
- Presenting a risk of harm to themselves or others.

The inclusion in a watchlist will be deemed strictly necessary to achieving the policing outcome and only when less intrusive means of location have proved unsuccessful.

Each deployment of Live Facial Recognition will be subject to a full Authorising Officer pre deployment authorisation report which will clearly define the strictly necessary argument for processing personal data, along with setting out clearly the case for the deployment's compliance with the College of Policing's Authorised Professional Practice of being targeted, intelligence led, time bound and geographically limited. That document will outline additional risk assessment and mitigations applied in addition to this DPIA.

The Deployment of LFR is driven by Norfolk and Suffolk Constabulary policing priorities and intelligence-led assessments, both of which determine locality and policing purpose. The locality and policing purpose then determine the composition of the Watchlist in line with the controls in the Norfolk and Suffolk Constabulary LFR Documents.

The individuals found on a Watchlist are there because there is a policing purpose to locate them that is driving the LFR Deployment. This may include those aged under 18, those under 13, a person with a disability or vulnerable adults where there is a policing need and it is deemed to be necessary and proportionate to locate and/or safeguard these people. Norfolk and Suffolk Constabulary LFR Documents outline considerations regarding expectations of privacy and outlines specific controls and safeguards to mitigate any impact on those with a protected characteristic(s).

Whilst the upper size of the Watchlist may be a limiting factor on occasion (where the necessity and proportionality case has been made out for more people than it is possible to add to a Watchlist), this is anticipated to be a very rare occurrence. It is also crucial to note that the technical potential size of a Watchlist does not drive Watchlist composition – intelligence, locality, policing purposes and policing priority do in line with Norfolk and Suffolk Constabulary strategic objectives as set out in the Norfolk and Suffolk Constabulary LFR documents.

Together, they may justify the necessity and proportionality of the particular Watchlist's composition and the need to deploy LFR using a Watchlist designed for the needs of that Deployment.

For those not on the Watchlist who are in an area where LFR is deployed there will be no impact or intrusiveness except where there is an Alert, whereby an officer will compare the images and if necessary, can speak with the identified individual. This means that there may be a reduction in stop and search. The signage and information around the target location means that individuals can choose not to be in the vicinity of the LFR.
It is recognised that exercising a choice not to be in a vicinity would be extra difficult when attending a protest or demonstration. The use of LFR can assist Norfolk and Suffolk Constabulary 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 the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting 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 weighed 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.

Passing the LFR system: LFR works by analysing key facial features of those passing the LFR system to generate a mathematical representation of them. This involves the processing of biometric data given the need to create Templates of everyone who passes the LFR system and compare them to those held on a Watchlist.

The courts have recognised the right of police to make use of a photograph of an individual. 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". Additionally, as the Surveillance Camera Code notes, an individual can, however, "rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place".

The position in relation to LFR was considered in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin).* The court recognised in that case the policing common law powers to use facial recognition technology were "amply sufficient" and that biometric processing of passers-by, whilst fleeting in nature, would be on the grounds of strict necessity to fulfil a law enforcement purpose as opposed to being based on consent.

The position was further considered by the Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058.* The Court of Appeal concluded:

"The short answer, in our view, to this submission is that the legal framework which regulates the deployment of AFR Locate does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary."

Consent would be entirely impractical to obtain during an LFR deployment and would undermine the law enforcement purpose underpinning the Deployment. The Court of Appeal in *Bridges* confirmed the Division Court's general findings on the legal framework but 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".

In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held in the case before it 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 "Where Question" and the "Who Question".

(a) The 'Where Question: Norfolk and Suffolk Constabulary LFR Documents answers this question, particularly the Norfolk and Suffolk Constabulary LFR SOP. In answering this question, in many instances, the need to locate a person 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).

(b) The 'Who' Question: Norfolk and Suffolk Constabulary address the 'Who Question' in its published Norfolk and Suffolk Constabulary LFR Documents, particularly at Section 6 of the Norfolk and Suffolk Constabulary LFR SOP. Norfolk and Suffolk Constabulary set the criteria that applies to govern the images that may be included on a Watchlist and in what circumstances. To ensure the Watchlist criteria is accessible and foreseeable, Norfolk and Suffolk Constabulary explain terminology such as 'presenting a risk of harm' and 'victims, persons with information and close associates' to ensure that these are 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.

Children/Vulnerable Groups: It is possible that there will be processing of children or vulnerable groups however if their Biometric Template does not generate a Possible Match no other details will be processed and this information will be deleted immediately. Where there is a Possible Match, the LFR Operator will be Alerted, and further manual checks will be carried out to identify whether that person is on the Watchlist. There is no automated decision making in the process.

Public protection: LFR has the potential to engage the wider public, not just those passing the LFR system. Whilst the wider public that do not pass the LFR system will not be engaged by having their personal data processed, the effective use of LFR to locate those wanted by Norfolk and Suffolk Constabulary and the courts serves wider public protection, community reassurance and safeguarding. This is prevalent when necessity and proportionality is considered as part of the process of adding people to a Watchlist. There is therefore a substantial public interest in enabling the Norfolk and Suffolk Constabulary to efficiently locate those wanted by it and the use of LFR as part of wider Norfolk and Suffolk Constabulary operational strategies to target criminals and reduce harm.

Technology: LFR is a relatively recent technology in law enforcement, the use of which is growing increasingly within and beyond law enforcement. It is also a technology that has been trialled and tested by the UK Police Forces in order to understand its utility as a policing tool and its algorithmic performance in an operational context.

The Norfolk and Suffolk Constabulary LFR Documents also provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing need to understand the performance of an algorithm, particularly in operational contexts and also offers Norfolk and Suffolk Constabulary a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, Norfolk and Suffolk Constabulary would be in a position to explore that further.

1.1 Please explain the aim, purpose and intended effect the project/process/system will have on: the force; the data subject; and the public, including benefits and disadvantages.

LFR technology is an operational tactic that helps Norfolk and Suffolk Constabulary stop dangerous people who are wanted for criminal offences. It helps keep communities safe.

As a police force, Norfolk and Suffolk Constabulary has a number of long-established policing responsibilities and powers derived from the common law which have been consistently recognised by the courts. Norfolk and Suffolk Constabulary is obliged to comply with the common law and statutory safeguards in delivering its policing operational duties, and relies on the common law to discharge a number of its duties. LFR can assist with Norfolk and Suffolk Constabulary duties to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice, and uphold national security in line with the objectives for LFR articulated in the Norfolk and Suffolk Constabulary LFR Policy Document.

Norfolk and Suffolk Constabulary objectives for LFR are further outlined in the Norfolk and Suffolk Constabulary LFR Documents, particularly within the LFR Policy Document.

Norfolk and Suffolk Constabulary has drawn extensively on the experience gained from partner UK police forces trials and the operational use to date to inform the future use of LFR. The Norfolk and Suffolk Constabulary view is that LFR is a valuable tool that supports keeping Norfolk and Suffolk safe for everyone.

One such partner force is Bedfordshire Constabulary. The Beds Police trials and use of LFR to date have shown the potential benefits of LFR as an important policing tool – its use has resulted in the arrest of wanted individuals and helped tackle crime in the areas in which it is used.

LFR technology can significantly improve the effectiveness of an officer's ability to locate wanted individuals. It can assist officers where traditional policing methods may struggle to yield results. An individual officer cannot possibly remember all of the faces of wanted persons on a Watchlist. Neither can an individual officer easily spot someone in a large crowd. LFR is a precision tool that improves the MPS's chances of picking out the person it is looking for.

LFR has a number of advantages over other systems currently used by Norfolk and Suffolk Constabulary such as CCTV. LFR allows the deployment of its resources more efficiently. For example, the LFR system will actively alert officers to the potential presence of individuals of interest to them rather than requiring larger numbers of officers to watch a busy CCTV feed. LFR has the capacity to assist officers where the number of people passing officers (or a CCTV system) makes identifications challenging (e.g. when the number of individuals to be identified is significant).

LFR also has a public protection, community reassurance and safeguarding role. For example, where the courts have issued a warrant for a person's arrest, many of these people pose a risk to public safety. These people may be located using LFR in circumstances where the officers would otherwise struggle and could not possibly be expected to remember the faces of all those currently wanted by the courts. The *Bridges* judgments recognised this rationale and supports this use case.

The ongoing effectiveness of use of LFR will be reviewed by way of a post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the Deployment. The LFR Documents reflect points arising from this process and lessons learned to date.

LFR's benefits are further outlined in the LFR Documents, particularly within the LFR Policy Document and LFR Legal Mandate.

Issues of concern as identified by third parties (to include the public, related Commissioners and Regulators and civil libertarian groups)
Proportionality and lawfulness – there are concerns that Deployments will limit or contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law. Also, the amount of personal data being processed is excessive and indiscriminate. Another concern is LFR may be used where it may be more appropriate to employ less intrusive methods.

Safeguards – There are concerns that there are insufficient safeguards around the use and Deployment of LFR.

Function creep – There are concerns that LFR will be used to monitor movements and action of the public beyond the scope of targeted Deployments or be used for covert surveillance.

Retention – there are concerns that all data captured during a Deployment will be kept as intelligence. There are also concerns that False Alerts may result in personal data being retained for longer than necessary.

Discretion – There have been concerns that there is too much discretion left to officers around the "who" and the "where" of Deployments.

Bias – There are concerns that the software algorithm may contain inherent bias with regard to the protected characteristics of race, age and gender. The human failsafe of an officer checking the image when a Possible Match is received is not sufficient to meet the Public Sector Equality Duty.

Legislation – It is acknowledged that there is always an opportunity to strengthen the legislative landscape for law enforcements use of emerging biometrics. Norfolk and Suffolk Constabulary have membership of the National Biometrics Board through which it will take on learning and develop its practices in accordance with legislation and policy as it emerges.

Public perception and expectations: A number of bodies have undertaken surveys relating to public awareness and perceptions of LFR. These surveys help inform us and its approach to LFR.

ICO: A report was commissioned by the ICO in January 2019 which indicated that there is strong public support for the use of LFR for law enforcement purposes:

- 82% of those surveyed indicated that it was acceptable for the police to use LFR;
- 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;
- 65% of those surveyed agreed or strongly agreed that LFR is a necessary security measure to prevent low-level crime; and
- 60% of those surveyed agreed or strongly agreed that it is acceptable to process the faces of everyone in a crowd even if the purpose is to find a single person of interest.

The public's support continues even if they were to be stopped by the police as a result of LFR matching them (erroneously) to a subject of interest. 58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.

Impact on force: The deployment of LFR can be a valuable policing tool that help forces keep the public safe an to meet our common law policing duty, which include the prevention and detection of crime, the presentation of order, and bringing offenders to justice.

Impact on data subjects: Should a person on the watchlist enter an LFR deployment area and an alert be generated, an officer will compare the images and if necessary, officers will speak with the identified individual. For those not on the watchlist who are in an area where LFR is deployed there will be minimal impact or intrusiveness as their biometric data will be briefly checked and deleted.

Impact on the public: There is an expectation on Suffolk and Norfolk Constabulary to bring offenders to justice, reduce criminality and make the Policing area(s) a safer place for people to live, work and visit. LFR technology allows Suffolk and Norfolk Constabulary to achieve those aims, but only where there is targeted, intelligence-led and both time and geographically limited rationale for doing so, ensuring that the argument for it being strictly necessary to process data in this way is met.

1.2 What categories of personal data will be processed? Provide an overview of the categories of

personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

Personal data which is already accessible and processed by the police (held in source system Athena) will also be processed in conjunction with the use of LFR. This may include but not limited to the name, date of birth and address of an individual. These details will not be included in the actual LFR Deployment of facial recognition technology but would be processed in the event of a Possible Match and therefore should be considered outside the scope of this DPIA.

Personal data in respect of individuals who are to be included in the Watchlist will include name, date of birth, occurrence numbers, photograph etc which are processed for compatible purposes in any event.

The categories of personal data processed in the course of an LFR deployment will comprise of:

- Images of individuals for inclusion in the watchlist
- Extracted biometric templates of individuals included in the watchlist
- CCTV images of individuals passing through the LFR zone of recognition
- Flagged matches
- Logs and records pertaining to consideration of matches and any engagement undertaken with individuals

1.3 Will special category data be used in the proposal? (Select all that apply)

☒ Race	☐ Trade union membership
☒ Ethnic origin	☐ Genetic Data
☐ Political opinions	☒ Biometric Data
☐ Sex life	☐ Sexual orientation
☐ Religion	☐ Health
☐ Philosophical beliefs	☐ None

1.4 Will it involve the collection of new information about individuals? Will the Force collect data that it has not previously collected or had access to?

☐ Yes
☒ No

If yes, please give details.

1.5 How many individuals will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects
☐ 100 to 1000 data subjects
☐ 1000 to 5000 data subjects
☒ More than 5000 data subjects

1.6 What categories of data subject are involved? (Please select all applicable categories below)

☒ Persons suspected of having committed or being about to commit a criminal offence

☒ Persons convicted of a criminal offence
☒ Persons who are or may be victims of a criminal offence
☒ Witnesses or other persons with information about offences
☒ Children or vulnerable individuals
☒ Employees (current and former)
☒ Other

If other then please provide further details below:
Deployments will be a real time capture of the biometric templates of any individuals who cross the path of the camera therefore a cross section of the general public including all categories will potentially be processed.
The watchlist will be complied from lawfully held images based on the criteria of the deployment.
It is possible that the personal data of individuals aged under 18 years, those under 13 years, a person with a disability or vulnerable adults will be processed where there is a policing need, and it is deemed necessary and proportionate to locate and/or safeguard these individuals.

1.7 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?
For example, can the aim be achieved by using less data or different types of data?
Are all categories of data necessary to achieve the aim?

LRF can be a valuable policing tool that helps forces keep the public safe and to meet their common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.
The following are illustrative examples of where LFR may assist Suffolk and Norfolk Constabulary achieve their policing purpose:

- Supporting the location and arrest of people wanted for a criminal offence
- Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders)
- Supporting the location of people about whom there is intelligence to suggest they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons deemed at increased risk, etc).
- Supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed.

LRF can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. The challenges presented in locating and arresting offenders should rightly be challenged and with the assistance of technology, more enhanced and cost-effective methods can be called upon to bring those responsible or suspected of offences more quickly to justice. Those data subjects added to a watchlist, will be subject to strict criteria and where less intrusive means have proven unsuccessful.

1.8 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

As explained above, LFR can have a significant impact in helping Suffolk and Norfolk Constabulary achieve their policing purpose by aiming to arrest those wanted for serious offending, for those who mean to cause serious harm and for those who may be at high risk of harm to themselves.

There is an understanding that LFR is a new technology and there may rightly be concerns from data subjects as to the intrusiveness of the technology. For those not on the watchlist who are in the area where LFR is deployed there will be no impact and minimal intrusiveness except where there is an alert, whereby an officer will compare the images and if necessary, can speak with the identified individual. The signage and information around the location means that individuals can choose not to be in the vicinity of the LFR technology. For those not on the watchlist who have their biometric data captured, the data is deleted immediately.

Potentially these categories of data may be processed which in turn may indicate an individuals age, gender and ethnic origin. FRT algorithms will be developed to eliminate or reduce any bias involving these categories as part of the Public Equality Duty and compliance with obligations arising from the Equality Act 2010 must be demonstrable. S149 states:

'A public authority must, in the exercise of its functions, have due regard to the need to:
eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act

a) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it
b) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.'
c) It should be noted that processing personal information as part of an FRT Equitability Evaluation will be detailed in a separate DPIA.'

Section 2 - Information Lifecycle

2.0 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal.

1. The Watchlist is created via a CSV file and corresponding Candidate Images which are saved in a secure folder within the force ICT domain - Images are typically imported in to the LFR application for each Deployment from Athena and the Police National Computer (PNC). Data may also be provided by other police forces and agencies associated with law enforcement and also from the general public.

2. The content of the folder is extracted into the LFR application via an encrypted USB drive onto a laptop that is not connected to the force ICT infrastructure and can be considered a 'black box' solution prior to Deployment

3. The collection of personal information is via two CCTV cameras connected to the standalone laptop/server.

4. The application 'extracts' a face from CCTV footage (known as a Probe Image) creates a Biometric Template and then compares it against a pre-defined Watchlist, every Candidate Image in the Watchlist will also have a Biometric Template created.

5. When the facial features from two images are compared the LFR application generates a Similarity Score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A Threshold value is set to determine when the LFR software will generate an Alert to indicate that a Possible Match has occurred.

6. Trained members of police personnel will review the Alerts and make a decision as to whether any further action is required. In this way, the LFR application works to assist police personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

2.1 Storage

Describe where and how the data will be stored.

The Watchlist is bespoke for every Deployment and the rationale for the make-up of the Watchlist must be intelligence-led, justified, proportionate and necessary, with the nature of the Watchlist recorded prior to each Deployment.

The Candidate Images and related Biometric Template are deleted immediately post Deployment and in any case within 24 hours.

The criteria for constructs of Watchlists for use with LFR must be approved by the Authorising Officer (the 'AO') and be specific to an operation or to a defined policing objective. Watchlists, and any images for inclusion on a Watchlist, must also be limited to the categories of image articulated in Force policy documents which are images of people who are:

a. Wanted by the courts; and/or
b. Suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where there are reasonable grounds to suspect an individual depicted to be committing an offence; and/or
c. Subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the Deployment; and/or
d. Missing persons deemed increased risk; and/or
e. Presenting a risk of harm to themselves or others.

Images are typically imported in to the LFR application for each Deployment from Athena and the Police National Computer (PNC). Data may also be provided by other police forces and agencies

associated with law enforcement and also from the general public. Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a policing objective and the proportionality of using such images on an LFR Deployment.

Where it is viable to do so without unduly impacting on the performance of the LFR application, Force policy documents should provide that suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by the Force, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of non-police originated image.

Non-police originated images should only be included in a Watchlist with the authorisation of the AO. The AO should also consider all the circumstances pertaining to the image and in particular the factors above. For the image of a missing person to be acquired from non-police systems, it needs to be provided and verified by Family or close friends and a written authority in Officers Pocket Notebook allowing Police to use photo for LFR purposes.

2.2 Use

Describe how the data will be used. Describe whether it involves new technology or novel processing.

The FRT software compares the extracted facial features with those contained in the facial images held on the Watchlist. When facial features from two images are compared, the FRT software generates a Similarity Score. A Threshold value is fixed to determine when the software will indicate that a Possible Match has occurred. Fixing this value too low or too high can, respectively, create risks of a high False Alert Rate (i.e. the percentage of incorrect matches identified by the software) or a high False Negative rate.

Additional information is also created in the form of metadata i.e. time, date and location. Where an individual is engaged by an officer following a Possible Match other details such as their name may be captured however this is out of scope of the LFR activity.

2.3 Recording

Describe the processes for recording the data.

The Watchlist is created via a CSV file and corresponding Candidate Images which are saved in a secure folder within the force ICT domain. The content of the folder is extracted into the LFR application prior to Deployment via an encrypted USB drive.

Force policy documents should also provide that the composition of Watchlists:

a) must be based on the intelligence case, reviewed before each Deployment to ensure that all images meet the necessity and proportionality criteria for inclusion, and the make-up of the Watchlist should not be excessive for the purpose of the LFR Deployment; and

b) must only contain images lawfully held by police with consideration also being given as to:

- the legal basis under which the image has been acquired; and

- the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk
- must only use images where all reasonable steps have been taken to ensure that the image:
    - is of a person intended for inclusion on a given Watchlist; and
    - is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist. Regard must be paid to the prospect of the LFR application generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken. Images should be imported into the LFR application immediately prior to
    - Deployment and no more than 24 hours prior to the commencement of the Deployment in order to ensure the Watchlist is current.

The LFR application will create Biometric Templates of the faces in the Watchlist. This will then use a live camera feed to scan faces of individuals in a designated area creating Biometric Templates of each to compare against those in the Watchlist.

The collection of personal information is via two CCTV cameras connected to the standalone laptop/server. The laptop is not connected to the force ICT infrastructure and can be considered a 'black box' solution. The application 'extracts' a face from CCTV footage (known as a Probe Image) creates a Biometric Template and then compares it against a pre-defined Watchlist, every Candidate Image in the Watchlist will also have a Biometric Template created. In doing so, the application does not save the live CCTV feed, only a particular face if a Possible Match is made against a Candidate Image along with a wider CCTV frame from which the Probe Image was extracted.

The CCTV feed will itself be saved. This processing is out of scope of this DPIA.

Not every person that is captured via the CCTV will be enrolled into the application. The face has to be of sufficient 'quality' to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include;

- Crowd density,
- Individual movements,
- Face angle; and
- Lighting.

It is the intention during each Deployment to allow the LFR application to enrol and therefore process as many individuals as possible, however it is worthy of note that processing that does not lead to an Alert will be momentary, and the image permanently deleted. No additional information will be attributed to the images of individuals enrolled into the LFR application. The application has a built-in audit trail functionality that ensures Probe Images that do not generate a Possible Match against a Candidate Image are not retained within it.

Any Biometric Templates which do not create a Possible Match against those on the Watchlist are deleted immediately. Where there is a Possible Match, this will generate an Alert which is displayed to the LFR Operator.

Interpretation of Watchlist categories:

'Further police action required.' This term will reflect the nature of the criminal investigation underway. Where it is lawful and necessary to do so, it may include the need to arrest the individual for further policing enquiries. On other occasions, the investigation may, for example, require details to be verified with an individual to progress the investigation. Proposed further police action will be specified and recorded in advance of the decision to include an image on a Watchlist and the action proposed will be in accordance with lawful police powers.

'Missing persons deemed increased risk.' This term will be subject to the College of Policing definition of medium risk (or above) contained in Missing Persons APP. That is the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public.

'Presenting a risk of harm.' This term will be informed by the intelligence case. This will need inform the AO as to how the individual presents a risk of harm and how:

a) Using LFR to facilitate their location is necessary to manage the risk of harm identified; and
b) Why it is necessary for the police to take action in order to manage the risk of harm.

The addition to the Watchlist will also need to be a proportionate response to the need to manage the risk of harm. Addressing the risk of harm in this context will need to have a legal basis under a policing common law power or another legal power. 'Harm' may include a risk of harm arising in relation to a person's welfare and/or a financial harm including as a result of fraud of other dishonesty.

2.5 Processors

Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?

No third party is being used, and data will not be processed outside of the UK.

2.5 Sharing

With which external organisation(s) is the data shared, what data is shared, and why?
Describe any sharing that will occur within Force
Outline any national and international sharing or processing.

The data will not be shared with any external organisation unless legally required to do so.

2.6 Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate.

Biometric data will be immediately destroyed if there is no match to data on the watch list, and within 24 hours if there is a match.
All CCTV footage generated from LFR deployments is deleted within 31 days, except where retained:

- In accordance with the MoPI, Criminal Procedures and Investigations Act 1996; and/or
- In accordance with Norfolk and Suffolk Constabulary complaints / conduct investigation process.

The watchlist data will be deleted within 24 hours.

2.7 Disposal
Describe the process for disposal of data, including when and how.

Any Biometric Templates which do not match those on the Watchlist are automatically deleted immediately.

Where there is a Possible Match this will generate an Alert, which is displayed to the LFR Operator. If a Possible Match is made three thumbnail images will be saved within the LFR application along with the related metadata. The first is the Candidate Image, the second is the face extracted from the CCTV and the third being the CCTV frame from which the Probe Image was extracted. The maximum retention period for Possible Match images and the related Biometric Templates is 24 hours although generally this information is deleted immediately post Deployment.

Watchlists and associated metadata are deleted immediately after Deployment or at latest within 24 hours.

LFR Operator and Engagement logs are retained in line with MOPI retention periods.
All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

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

2.8 Audit
If applicable, is the system auditable? Does it have a function to pull reports to audit access/usage of the system?

Following the conclusion of any Deployment the force will apply learning including evidence of effectiveness in similar operational scenarios and to carry it forward to subsequent Deployments to ensure the use of LFR on each successive occasion is truly beneficial, in particular to the public. The processing will also take place against the requirements of the Surveillance Camera Code of Practice of which one of following principles is that "there should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published".

The application has a built-in audit trail functionality that ensures Probe Images that do not generate a Possible Match against a Candidate Image are not retained within it.

Technical systems and standard operating procedures help ensure that data is properly retained or deleted. A post-Deployment review process and associated internal audit function is used to identify lessons for the future and periodic audit provide assurance.

Section 3 - Security, Access and Transfers

3.0 What security measures will be in place to protect the data? Describe the physical, organisational, technical security measures that will be in place.

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. Access to the LFR system is limited to those with a need to use it.

Images are transferred onto the LFR system via an encrypted USB device. Access to the USB stick containing the Watchlist is limited to those with a need to use it.

The data is held securely on the system accessible via the operating Police forces computer system. The data held on the operating police computer systems is not specific to LFR (it provides LFR with the information needed to compile and generate a Watchlist and relates to policing information generated following LFR Alerts). Norfolk and Suffolk Constabularies have their own policy on retention, review and disposal that applies to this information, including the need to hold and review policing information in accordance with MOPI and CPIA (as applicable).

3.1 Access

Who will have access to the system? e.g. supplier, staff within the force, third parties.	What is the purpose of the access? e.g. carrying out work tasks, supplier needs for troubleshooting purposes	How will they access the data/system? e.g. remote access, individual log in, etc.	What level of data will they have access to? Partial data, all data etc. If partial, please specify.
LFR Operators (police officers and staff)	To carry out the operative capability of the LFR equipment	Individual login	Access to data uploaded from encrypted USB to LFR software on standalone laptop by trained Police Officers or Staff.
Staff within the force	To upload onto an encrypted USB	Will not have access to the standalone LFR software and data	Designated staff will have access to the encrypted USB

3.2 Data Transfers

Transferring data outside the UK but within the EU?

☐ Yes

☒ No

If yes, please give details.

Transferring data outside the EU?

☐ Yes

☒ No

If yes, please give details.

3.3 Assets

Please give details of the assets that you intend to use.

Hardware ☒ CCTV cameras, Laptops, Modified police vehicles

Software ☒ Live Facial Recognition software

Networks ☐ Norfolk and Suffolk Constabulary Network

Hardcopy/Physical e.g. paper ☐

Other ☐

Section 4 - Lawful Basis

4.0 Lawful Basis

To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Necessary for a law enforcement purpose

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes):

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority

4.1 Lawful Basis – Special category data

If processing special category data you must have identified a further lawful condition

Operational Data:

The processing is strictly necessary (please tick to confirm) ☒

AND

One of the following conditions applies (select from the list):

Statutory Purpose

Administrative Data

It is necessary for one of the following conditions (select from the list):

Choose an item.

OR

It is in the substantial public interest (tick to confirm) ☒

AND for the following purpose:

Statutory function

Section 5 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

5.0 Do you intend to consult data subjects?

☐ **Yes**
If yes then outline your plan in **Section 5.1** below together with details of consultation with other stakeholders.

☒ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 5.1** below.	The data subjects effected by this proposal will be people who are added to a watchlist for a specific policing purpose, which will generally involve the deployment trying to assist in on of the following: • Locate wanted persons • Preventing disruption in the area by identifying persons who may cause harm • Locate people who may pose a risk of harm to themselves or the wider public • Support targeted preventative policing activity to prevent criminality and disorder. If it were possible to seek the views of these people, this proposed tactic would be negligible. However, all appropriate documentation relating to the deployment of live facial recognition will be published on the Norfolk and Suffolk Constabulary website in advance of deployment.

5.1 Consultation Action Log
Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The general public
- Union representatives
- Information Assurance
- Information Rights
- Force Legal Services
- Partner agencies
- Data processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome
Bethany Mortimer – Head of Joint Information management.	19/02/26	Via Teams call.	Progression of documents in compliance with force policy.
IAG Strategic Board	03/02/26	Via teams conferencing.	Presentation delivered to the group explaining LFR, it's uses, watchlist creation and legal documents produced.
NPCC – National Biometrics Function	23/10/2024	Teams meeting	Advice provided on required documentation,

			processes, communication strategy and deployment.

Section 7 - Full Risk Assessment	
Identify and Assess Risks In this section you must detail all data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. Please see Annex A where you can find the Data Protection Principles which may help you identify risks.	
Examples of **risks to individuals** include**:** • Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional, or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.	Examples of **corporate risks** include: • Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations

You should identify **solutions** such as:

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct
- Restricting access to data
- Training staff to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk Score**	**Mitigation/ Solution**	**Result**	**Residual Risk**
	1 - Remote 2 - Possible 3 - Probable	*1 - Minimal 2 - Significant 3 - Severe*	*High Medium Low*	*Describe the mitigation and whether it will be implemented*	*Is the risk: - Eliminated - Reduced - Accepted*	*High Medium Low*
As a result of the Watchlist being deleted after 24 hours the force may be unable to comply with a subject access request from a data subject resulting in complaints, reputational damage and potential financial claims.	1	2	Medium	The Watchlist can be re-engineered. This can now be achieved via Athena 'back-end' database by recording the nominal number of an individual extracted into a Watchlist for any given date	Eliminated	Low
There is a risk that intervention may take place as the result of a False Alert due the Threshold value for a Similarity Score being set too low or too high resulting in reputational damage, potential enforcement action and financial penalties, loss of public trust and increased volumes of complaints.	1	3	High	The LFR Operator will complete the Adjudication prior to any Engagement.	Reduced	Low
As a result of the scope of a Deployment there is a risk that fair processing information may not be	2	2	Medium	A communications strategy will be in place prior to any Deployment to ensure that all	Reduced	Low

widely available to members of the public resulting in them not being informed of the processing of their personal data resulting in a potential data breach, increased complaints, court cases, enforcement action and reputational damage.				available means of communicating the fact that a Deployment will/is taking place via various channels including digital and physical, and information is available to the public on why Deployments are effective to ensure that individuals and the public are confident that the decisions made to deploy and continue to operate LFR are based on firm evidence and transparent analysis. The use of cameras will also be assessed against the Surveillance Camera Commissioner's Camera Code (as required under s29 of the Protection of Freedoms Act 2021).		
As a result of the nature of LFR there is a risk that Deployments may limit or contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law resulting in potential legal challenge, financial claims and increase in complaints.	2	2	Medium	The assessment prior to any Deployment of LFR will determine whether interference with these rights is necessary, proportionate and lawful and whether there are less intrusive methods which could be employed. Full, robust justification will be documented prior to any Deployment.	Reduced	Low
As a result of issues to narrow the scope of the Watchlist there is a risk that the images included for a Deployment may be excessive.	2	2	Medium	The assessment prior to any Deployment will include the requirements and justification of the inclusion of images in	Reduced	Low

				the Watchlist to ensure that the strict necessity threshold is met and there is a reasonable expectation that those individuals will be in the vicinity of the Deployment of LFR. Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use.		
As a result of limited availability of images for testing the software there is a risk that bias may not eliminated in the algorithm resulting in a disproportionate number of individuals with protected characteristics being identified in False Alerts leading to potential legal challenge, financial claims and increase in complaints.	2	3	High	Assurances around the testing conducted by the software supplier are required in the contract and is continually monitored to ensure that any potential bias in the use or development of the technology is identified and rectified as part of the public sector equality duty and through assessment by academic institutions, technology vendors and government opinion. Watchlists will also be checked to ensure that gender or ethnicity is not unfairly represented. Equality Impact Assessments will be completed and regularly reviewed against legal developments.	Reduced	Low
As a result of the wide-ranging capability of LFR to process large amounts of personal data there is a risk that the processing of personal	2	3	High	The assessments prior to a Deployment will consider and document why less intrusive methods are not appropriate	Reduced	Low

data may be excessive resulting in regulatory action.				and justifying the use of LFR based on intelligence.		
There is a risk that LFR may be deployed during covert surveillance resulting in potential unlawful processing of personal data – potential court cases, loss of opportunity to prosecute, increased complaints, reputation damage and potential regulatory enforcement action.	3	3	High	An additional legislative safeguard is any covert surveillance will require authority under the Regulation of Investigatory Powers Act 2000 as per arrangements for any covert surveillance.	Reduced	Low
Due to the similarity in requirements for LFR there is a risk that each Deployment and Watchlist is not subject to a full assessment documenting the rationale for inclusion of images 'the who', the scope of the location, duration 'the where' and whether the strictly necessary threshold has been met resulting in a risk of unlawful processing and breaches of the Data Protection Act 2018 which may lead to financial claims and penalties, court cases.	1	2	Medium	The LFR Policy requires a suite of documents to be completed prior to any Deployment of LFR within the force area -or as soon as possible in urgent cases. These documents require authority to deploy and documents all justification, criteria and detail around necessity, effectiveness and purpose of Deployment to ensure it is targeted; intelligence led and time limited	Reduced	Low
As a result of potential incomplete deletion exercises there is a risk that Watchlists may be compiled using custody images which should have been deleted from police systems in line with established retention and deletion procedures or from images of uncertain	2	3	High	Watchlists will be limited in size and will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. No Engagement will be made without checks being made on	Reduced	Low

provenance where accuracy may be an issue (e.g. sourced from social media) there is a risk that these may lead to an unjustified Engagement and potentially cause unwarranted and unjustified damage and distress to individuals.				Possible Matches without manual intervention to reduce any damage and distress.		
As a result of different scenarios in which a person may be reported as missing there is a risk that the use of LFR to locate that person may not meet the strict necessity threshold and may be unlawful resulting in potential legal challenge, complaints and financial penalties or regulatory enforcement action.	2	3	High	Where a Deployment is being used to locate a missing person a strict necessity test will be conducted to determine the degree to which the missing person is vulnerable and whether there is sufficient intelligence to indicate that the individual may be in a particular area at a particular time. This will need to be signed off by an officer of the required authority. For the image of a missing person to be acquired from non-police systems, it needs to be verified by Family or close friends and a written authority in Officers Pocket Notebook allowing Police to use photo for LFR purposes.	Reduced	Low
Where the force has not completed an appropriate policy document there is a risk that it will be in breach of section 42 of the Data Protection Act 2018 resulting in potential regulatory enforcement action and/or financial penalties.	1	3	Medium	The force will have in place appropriate policy documents for LFR processing under Part 2 and Part 3 of the Data Protection Act 2018	Reduced	Low

As a result of inconsistent guidance around the use of LFR there is a risk that officers may exercise too much discretion around inclusion in the Watchlists and the location of the Deployment resulting in excessive and unlawful processing of data which may lead to legal challenge, complaints and potential enforcement action.	3	3	High	Our LFR Policy stipulates documentation and authority required for a Deployment ensuring consistency and oversight for each Deployment, in addition to the College of Policing LFR APP and SCC Codes of Practise that must be adhered to.	Reduced	Low
There is a risk that officers involved in the Deployment of LFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the Deployment of LFR and potential breaches of the DPA'18 which may result in enforcement action, legal action and financial penalties.	2	3	Medium	As part of the LFR training appropriate data protection training will be provided.	Reduced	Low
As a result of lack of training and awareness there is a risk the data entered onto the Watchlist is not treated within the correct Government Protective Marking Scheme (GPMS) resulting in adequate protection when handled and potential loss and damage.	1	1	Low	All staff/officers are trained in respect of the GPMS. Officers compiling Watchlists will perform this task in a secure environment to which the public do not have access. All Watchlists are appropriately stored prior to the operation and are deleted after the Deployment.	Reduced	Low
As a result of lack of training and awareness there is a risk that the	1	2	Medium	Officers/Staff compiling the Watchlists are briefed in	Reduced	Low

Watchlist or other data generated by the LFR application is unlawfully disclosed to third parties				respect of Watchlist circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, deployable officers and technical support staff. Any action following an Alert may involve Norfolk and Suffolk Constabularies working with other police forces, law enforcement bodies and other agencies to assist us in discharging its common law policing powers. This action will not require the sharing of biometric data but may require us to share personal data, as it would for any investigation, in accordance with our routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect the LFR application and the USB used to import the data into the LFR application.		
As a result of technical failure there is a risk that the equipment will not function correctly resulting in False Alerts or failure to identify Possible Matches resulting in potential damage and distress or threat risk and harm to others.	1	3	Medium	The technology has been trialled and tested by Norfolk and Suffolk Police, who will be operating LFR equipment and resource. NEC algorithms have also been evaluated by NIST and Norfolk and Suffolk Police pays regard to these findings.	Reduced	Low

				An LFR System Engineer, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters and reduce generation of the False Alert Rate to below 0.1% will be on call if technical assistance required. All relevant information is logged for audit purposes. Logs are kept by the Gold, Silver and LFR Operator and LFR Engagement Officer. Norfolk and Suffolk Constabulary LFR Documents also outline points relating to the LFR application to ensure that it is used in a way that maximises its effectiveness. They also place responsibility on the Silver Commander and LFR Operator to continually monitor and review the system's performance. The Gold and Silver Commanders are obligated to stop the Deployment, should the Deployment fail to meet the requirements of the DPA 2018 at any point.		

				The ongoing effectiveness of Norfolk and Suffolk Constabulary use of LFR is reviewed by way of the post-Deployment review process. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool.		

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Annex A

Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Force systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to Information Rights.