DATA PROTECTION IMPACT ASSESSMENT

This document enables you to complete a full Data Protection Impact Assessment (DPIA), if your Screening Form indicates that one is required.

Within the form below, you will find further clarification and assistance where you see a '?'.

Please also refer to the ICO guidance when completing this form.

How to complete this form?

In this stage of the DPIA process you must provide full details about the context, necessity, proportionality and risks associated with the proposal. It will supplement the information provided in the DPIA screening document.

The aim of this process is to identify and mitigate risks and to consult the Information Commissioners Office (ICO) (before processing commences) where residual risks to individuals are high.

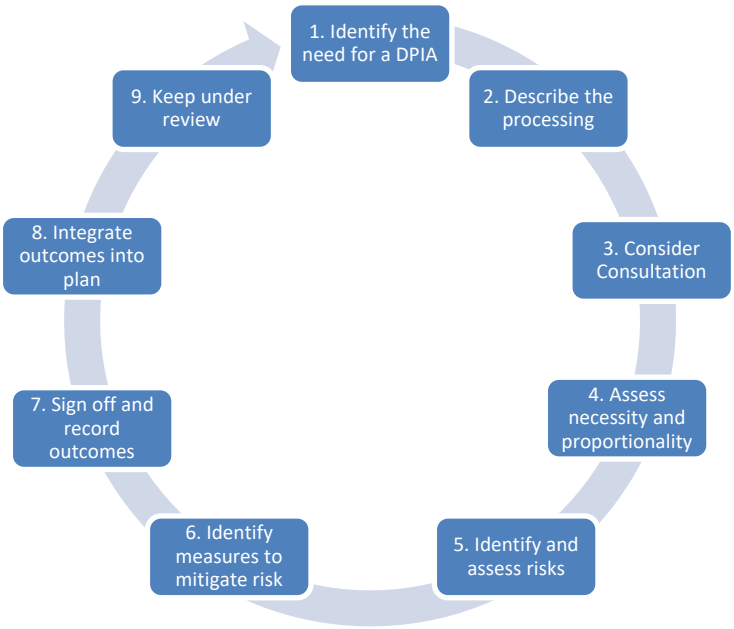
Data Protection legislation and the ICO set out essential requirements that must be addressed within a DPIA. These are incorporated into the form so it is vital that you fully complete every step (where relevant).

Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.

If you require advice or guidance, please contact the Data Protection Officer on dataprotectionenqs@nthwales.pnn.police.uk

In the event of a residual risk remaining 'high', the Head of Department/Information Asset Owner must refer this DPIA to the Data Protection Officer (DPO) on dataprotectionenqs@nthwales.pnn.police.uk and then following the DPOs advice, the DPIA will be referred to the Chief Information Officer/SIRO to accept the risk prior to referral to the ICO.

Below is an example of the DPIA lifecycle:



DATA PROTECTION IMPACT ASSESSMENT (DPIA)	
Project Proposal Name:	Use of live facial recognition technology on Mutual Aid from North Wales Police
Head of Department/ Information Asset Owner[?]:	ACC Chris Allsop
Designated Business Lead/Project Manager:	C.I Arwel Hughes
Date on which system/initiative expected to commence:	21/05/2024
Date sent to Head of Department/Information Asset Owner for assessment:	DD/MM/YYYY
Date assessment completed:	DD/MM/YYYY
If any residual risks remain High	
Date sent to Data Protection Officer:	DD/MM/YYYY
Date sent to CIO/SIRO:	DD/MM/YYYY
Date sent to ICO:	DD/MM/YYYY

Step 1: IDENTIFY THE NEED FOR A DPIA
1.1 Using the DPIA screening document, summarise the need for a DPIA (Include which screening criteria flagged the processing as likely to be high risk).

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed 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 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:

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).

The NWP 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.

As a general rule, a watchlist will be drawn from police-originated imagery, held on NICHE RMS.

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.

The NWP LFR Policy and SOP provides considerations relevant to the locations NWP may select to deploy the cameras when using them for LFR.

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

Feature extraction: Taking the detected face the software automatically extracts facial features from the image, creating the Biometric Template.

Face comparison: The LFR software compares the Biometric Template with those held on the Watchlist.

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.

Although not retained, the LFR technology does create new information about individuals, as it obtains their biometric data to match against a police-originated watchlist.

Additionally, with relation to the screening tool, it checks boxes 1 – 7, and as it is A.I, and new technology to be used by NWP, a full DPIA is required.

1.2 Project aims and purpose? • *What do you want to achieve?* • *What is the intended effect on individuals?*	Live Facial Recognition (LFR) is used by North Wales Police as a precision crime-fighting tactic to locate people who are wanted for criminal offences and helps protect the most vulnerable in our society. More detail about how LFR works and how NWP uses it can be found in the policy and standard operating procedure. LFR helps us locate those on a Watchlist, by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist of Candidate Images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. Watchlists composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment. LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in

	order to identify Possible Matches against persons of interest to Law Enforcement Agencies. Where the LFR application identifies a Possible Match, the LFR system flags an Alert to a trained member of personnel who then makes a decision as to whether any further action is required. In this way, the LFR application works to assist NWP personnel to make identifications rather than acting as an autonomous machine based process devoid of user input.
1.3 Benefits of the processing • *What are the benefits to the organisation, individuals, public?*	NWP uses LFR technology supplied by South Wales Police (SWP). This is on a mutual aid basis, where the technology is operated by SWP, but under the authority, direction and control of NWP. LFR has been trialled by SWP over a period of six years. Whilst NWP is its own law enforcement entity, we are aware of the results of these trials, and NWP believes that LFR is a valuable precision policing tool that can assist NWP to keep the public safe and to meet its 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 NWP with its policing purposes:- a) Supporting the location and arrest of people wanted for criminal offences; b) Preventing people who may cause harm from entering an area (e.g. under football banning orders); c) Supporting the identification 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, sex offenders etc.); d) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.

	Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. NWP is conscious that the use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing. It is therefore incumbent on NWP to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR. The use of LFR as a tool to locate Persons of Interest to NWP will be considered alongside other policing tools and tactics. Consideration will be given as to the effectiveness and intrusiveness of other viable methods that might produce the same result, with the least intrusive, viable method being adopted to progress an investigation.

Step 2: DESCRIBE THE PROCESSING AND FLOW OF INFORMATION

This section outlines the **nature**, **scope**, and **context** of the processing.

Please describe how and why you plan to use the personal data in as much detail as possible, including reference to the high risk processing identified in the screening.

2.1 Nature of the processing

2.1.1 Stage of processing	Description
Collection Where does the data originate from (sources), who will collect it, how will it be data obtained and how often?	The data will come from two sources – the data placed upon the watchlist, and the data obtained from the LFR system reading the faces of people who pass the cameras. In relation to the watchlist, typical deployments undertaken by South Wales Police have resulted in Watchlists of between 500 – 700 images however volumes will vary according to the necessity and proportionality for inclusion for each deployment. The limit is currently 2,000 images. It is not anticipated that

	NWP will exceed these figures. As initially this is a pilot, this will be reviewed post-deployment. The only source of the images for the watchlist at this stage of NWP's use of the LFR system will be images obtained via NICHE RMS. In relation to the individuals who pass the cameras, the exact number of individuals whose faces will be processed by the LFR cameras is unknown but is likely to be high volume. The geographical area will be determined by the purpose of the Deployment however the intention is to focus LFR overtly over a distinct geographically limited location or event which is relevant to the force area. The Authorising Officer will define the date, time, location and duration the deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the deployment. Whilst LFR may be used at locations across Nouth Wales, any Deployment will be limited to a specific location using hardwired cameras linked to the LFR application. The locations used will be based on the intelligence case to deploy LFR, the requirements of the LFR application and considerations relating to privacy that may attach to a particular area (as more particularly outlined in NWP LFR Legal Mandate and NWP LFR SOP). These controls assist the public and decision-making officers to understand LFR and foresee where it may be used.
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	**The data upon the watchlist will be matched against biometric data captured by the LFR cameras.** **Watchlists** Those included in the watchlist will be individuals suspected of criminality and who are wanted by the courts and police; individuals who may pose a risk to themselves and others; and individuals who may be vulnerable.

	There is a reasonable expectation that personal information will be processed for the fulfilment of operational police duties including: • Protection of life • Preserving order • Preventing the commission of offences, and • Bringing offenders to justice. Where it is necessary, proportionate, in pursuit of a legitimate aim and in accordance with the law. The Authorising Officer must be satisfied by the steps taken to ensure the composition of the Watchlist is not excessive and only includes those who need to be located by NWP using LFR on a strict necessity basis. The LFR Operator has the ability to delete images from the Watchlist and will record such action in the operator log. **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. Each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be aged under 18-years-old and under 13-years-old. Given the potential for System Factors relating to age, specific regard needs to be given to the importance of locating those aged under-18 on a risk-based approach in line with the NWP documents, with a particular focus on ensuring the necessity case is fully made out. If LFR is to be used to locate a person aged under 13-years-old, specific regard should be given to anticipate LFR application

	performance issues. Specific advice must (at this time) be sought from the SWP LFR team (as the team providing mutual aid) prior to seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO.
Access Describe who has access to the data throughout the life of the processing.	Regarding the watchlist composition, this will be completed by North Wales Police employees, using a pre-determined script to pull images from RMS. These will be trained and vetted NWP personnel. Regarding the general LFR application, the only persons with access to it will be trained SWP personnel, who are vetted and cleared to at least MV/SC level.
Processors Describe the use of processors. If a third party is used, is a contract in place to regulate the relationship? Will any personal data be processed outside of the UK or the EU?	South Wales Police will be a third party used to process data. They are a trusted partner UK policing entity. Our agreement with them will be covered under a data processing agreement, which will consider safeguards in place regarding the following: DPA Part 3 – APD on sensitive processing for law enforcement purposes. GDPR article 30, 9 - APD – processing of special category data under part 2 DPA 2018 and Article 9 general data protection regulation. The use of LFR technologies is governed by a number of codes of practice including those applying to the police such as PACE. In particular the use of LFR is covered in the twelve principles laid down in the Surveillance Camera Code of Practice, to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras applies to their use by the police and other authorities. The Surveillance Camera Code of Practice has the following principles:

	1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. 2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. 3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints. 4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. 5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them. 6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once its purpose has been discharged. 7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes. 8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards. 9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

	10. 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. 11. When the use of a surveillance camera system is in pursuit of a legitimate aim and a pressing need, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value. 12. Any information used to support a surveillance camera system which matches against a reference database for matching purposes should be accurate and kept up to date. South Wales Police will be responsible for providing training of South Wales Police officers and staff involved in LFR Deployments, and they will provide specific briefings to North Wales Police officers deployed to assist. The training helps ensure role specific: 1. familiarity with SWP LFR Documents; 2. knowledge of Deployment processes; 3. understanding of the lawful processing of personal data in accordance with the Data Protection Act 2018; 4. understanding the scope of the Regulation of Investigatory Power Act 2000; 5. knowledge of police powers and how they may apply when responding to Alerts; 6. knowledge of how to configure the LFR application to maximise system performance, and how to minimise impact on others; 7. understanding of the characteristics of the LFR application that affect the likelihood that an Alert is reliable.
Sharing Will you be sharing the data with anyone? If so, what will you share, why, and who will receive it? (Sharing could be external or internal to the organisation, national or international).	The data generated by North Wales Police in the form of our generated watchlist will be shared with South Wales Police to allow upload to the LFR system. South Wales Police is a trusted law enforcement partner. The sharing is necessary for the prevention and detection of crime, and for the location and detention of outstanding

	suspects, wanted people, and in line with the police's common law objectives and obligations under Article 2 of the Human Rights Act. In relation to other organisations, information will only be shared where necessary for a policing purpose on a case by case basis therefore no agreement is necessary. South Wales Police have a contract in place with the algorithm supplier for the LFR technology. The supplier does not have routine access to the software and algorithm supplied to SWP and do not act as a data processor for the purposes of this DPIA.
Review, retention, disposal Describe your plan for review and retention (e.g. how long you will keep the data), linking to the organisations' retention schedule where appropriate. Also, describe the process for disposal of data, including when and how.	**Retention:** Particular to the LFR Application **Biometric Templates – no matches** Any Biometric Templates which do not create a Possible Match against those on the Watchlist are deleted immediately. **Possible Matches** 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 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** Deleted immediately after Deployment or at latest within 24 hours **LFR Operator and Engagement Logs** Retained in line with the MOPI retention periods. Source System – Niche Record Management System

	Please refer to Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4) Non-conviction – upon request Group 1 or 2 (Public Protection Matters & sexual, violent or other serious offences respectively) – 10 years upon request then review Group 3 (all other offences) – 6 years upon request then review Group 4 (missing persons) – 6 years then review All other personal data will be stored in accordance with MOPI standards. Group 1 - subject is 100 years the review Group 2 – 10 year clear period then review Group 3 – 6 year clear period Group 4 (missing persons) – 6 years then review
Security measures Describe how you will keep personal data secure.	The watchlist images will be placed upon an encrypted USB stick, which can be facilitated by the data protection and information assurance office, and then uploaded on to the LFR application. Two types of access will be available to the application – 'user' and 'administrator' access levels Access is only granted to users following completion of training. The application has an in built and robust audit file log CSV file (hashed). Each LFR Operator will be given a username and password which they will be forced to change on initial use of the application - 'Active Directory' strength of eight characters to include upper and lower case as well as being alpha numeric. Local network passwords are security protected. The application is non-networked and non-configured to extend to the cellular network – essentially an additional geographical protection.

	The LFR application is 'closed' and not connected to other NWP systems or the internet. As a contingency against the technology failing and requiring the LFR Operator to wipe and reset it the encrypted USB memory stick is retained with the LRF Operator under the end of the Deployment meaning that they are able to reimport the watchlist to the rebooted LFR application enabling the Deployment to continue. The LFR uses an independent system to the current SWP technical architecture with 2 layers of password protection to access the application. The system is physically protected when in use. Images are transferred onto the LFR application via a USB using an AES-CBC 256-bit full disk hardware encryption engine that is further protected by pass number access. Access to the USB stick containing the Watchlist is limited to those with a need to use it. The data upon the LFR system is then held securely on police systems accessible to officers and staff which is fundamentally permission based. Officers leaving the SWP LFR team (the team operating the LFR equipment on behalf of NWP) automatically have their account disabled and therefore would no longer have access to the information.
2.1.2 Storage and Assets Describe where and how the data is to be stored including the assets you intend to use.	
Asset	**Description**
Hardware	The CSV file is imported onto a standalone terminal not connected to the internet, accessible only via the vehicle where the system is operated. At the end of each deployment (day) the system is wiped. At the start of the next deployment (day) the CSV file is re-imported.
Software	Automatically deleted and subsequently manually deleted by the operator at the end of TOD. Post deployment report is made to provide figures regarding alerts and faces seen
Networks	Vehicles operate a local network, though there is no remote access, internet capability or external access. Configured within the vehicle, via a single four-way switch and those ports are

	only accessible within. Two ports taken up by camera, one port by terminal, and fourth one unused but only accessible from inside the van.
Hardcopy/paper	Not applicable
Any other relevant assets	USB stick – encrypted to force standard.

2.1.3 Diagrams and tables

If you have a diagram or table which describes or demonstrates the processing (and information flows), please include it below.

1) LFR law enforcement purpose identified, safeguards considered, LFR deployment provisionally authorised by NWP NPCC Team.

2) Consultation made with providing force, and authority given for Mutual Aid to be provided to NWP.

3) Deployment authorised, and Watchlist selected;

4) Notification of deployment, and signage deployed;

5) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist;

6) If a Possible Match is found in a Watchlist, the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the Watchlist are presented to the LFR Operator / LFR Engagement Officer for human review;

7) The LFR Operator / LFR Engagement Officer will consider the Alert, noting the System, Subject and Environmental Factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is engaged;

8) cancellation of authority for the LFR Deployment and post-deployment evaluation

NWP Standard Operating Procedure provides a greater level of detail about the processes involved in the deployment of LFR by NWP.

2.2 Scope and context of the processing

2.2.1 Will the processing involve law enforcement? data or general data?

(Please select below)

☒ Personal data processed for law enforcement purposes

☐ Personal data processed for general (non-law enforcement) purposes

2.2.2 What categories of individuals will be 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

☐ Organisations' staff (current and former)

☒ Other

If other, please provide further details below:-

Click here to enter text.

2.2.3 What types of personal data will be processed?

Provide an overview of the categories of personal data that will be processed, for example: names, DOB's, addresses, vehicle registration plate number, 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 Niche RMS) 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.

2.2.4 How many data subjects 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

2.2.5 Will you be processing any special category or criminal data?

(Please specify one or more answers below)

☒ Race or Ethnic origin	☐ Trade union membership
☐ Political opinions	☒ Genetic or Biometric Data
☐ Religious or Philosophical beliefs	☐ Sex life / Orientation
☒ Criminal convictions/offences	☐ Health

2.2.6 Will the processing include data about children or other vulnerable people?

Please provide details in the text box.

☒ **Yes** ☐ **No**	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 to be necessary and proportionate to locate and/or safeguard these individuals.

2.2.7 Your relationship with the individuals:

Describe your relationship with the individuals who are subject to the processing. Are they likely to expect the processing? Outline the extent to which they will have control over their data.

The individuals processed under these circumstances will be previously known to the police, with their images obtained from lawfully held police images. They will in be aware that the police hold their images. They are able to request the deletion of their images from police databases in line with national guidance.

2.2.8 Has personal data been processed in a similar way previously?

Please provide details in the text box.

☒ **Yes** ☐ **No**	The personal data will already have been processed by the police, as the photograph is derived from the subject's record on RMS

2.2.9 Have you considered any approved codes of conduct, certification schemes or codes of practice?

☒ **Yes** ☐ **No**	The use of LFR technologies is governed by a number of codes of practice including those applying to the police such as PACE. In particular the use of LFR is covered in the twelve principles laid down in the Surveillance Camera Code of Practice, to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras applies to their use by the police and other authorities.

Step 3: CONSULTATION

You should consider seeking the views of data subjects unless there is good reason not to. If the processing involves staff data, you should consider consulting them or their representatives. Consideration should also be given to consulting with Information Assurance (IA) for any new systems (that process personal data) and the audit capabilities within that system.

3.1 Do you intend to consult with data subjects?

☐ **Yes**

Outline your plan in **Section 3.2** together with details of consultation with other stakeholders.

☒ **No** Outline rationale[?].	The reason for checking no in this instance is that this is not new technology used by policing, it has been used and trialled by South Wales Police for 6 years, and we are using their technology on Mutual Aid. Following the pilot in NWP, full consultation with the NWP Ethics Committee will be instigated, along with consultation with community groups and key stakeholders. In addition, the public within North Wales have demonstrated broad support for the use of Facial Recognition technology through a recent study undertaken by Bangor University. A summary of the consultation work completed by South Wales Police in relation to this subject, which adds a layer of assurance, is as follows: 1. Information Commissioner's Office – Advice and guidance was received from the ICO following the court case –(*Edward Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058*. This took the form of a guidance document called 'facing the camera'. The recommendations within this have been considered and incorporated into NWP policy and SOP. 2. In 2019 the ICO commissioned a report on use of LFR for law enforcement purposes in which the following public opinions were obtained: • 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 holds up 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. 3. Defence Science and Technology Laboratory (DSTL) – With the provision of guidance on procurement, testing and deployment of the technology, along with advice around academic documentation supporting the proof of concept of the product. They remain a critical friend to the project.

	4. Home Office Biometric Programme (HOBs) – Additional guidance in support of the above from the HOB lead on PIA's. 5. South Wales Police Independent Ethics Committee – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities. 6. The Metropolitan Police – Professional discussions around lessons learned over previous deployments, particularly the Notting Hill Carnival in the pursuit of a best practice model across forces. 7. Leicester Police – Professional discussions over their previous use of slow-time recognition functionality in the preparatory phase of SWP project implementation. 8. National Police Chiefs Council – Professional discussion and advice over the development of the project in its phases and the use of custody images. 9. The Surveillance Camera Commissioner/Biometric Commissioner – Professional discussion over project proposals and implementation. The SCC Code of Practice also states that an individual "can rightly expect surveillance in public places to be necessary and proportionate with appropriate safeguards in place". The Code and the guidance 'Facing the Camera' has been considered as part of the DPIA. Deployments of LFR also incorporate the SCC's checklist. 10. The College of Policing –LFR APP 11. Police Digital Service – Professional discussions over system developments against a desired national rollout picture of the future. 12. The National Physics Laboratory – Professional discussions integrating academic research into the policing technology, the ethical dilemmas associated with it and its deployment. This has resulted in the production of a research paper: 'Facial recognition technology in law enforcement - Equitability study' This study examined whether the concerns of equitability within facial recognition technology. 13.Strategic Facial Matcher (SFM)– Guidance in support of new platform anticipated 2024. 14. Ada Lovelace Institute – a report commissioned in September 2019 indicated that public support for LFR would be conditional on a demonstrable impact on reducing crime – 71% agreed with the statement

	"the police should be able to use facial recognition on in public spaces, provided it helps reduce crime". 15. The London Policing Ethics Panel (PEP) – an independent body set up by the mayor to provide advice on ethics, which produced a report on the LFR trials conducted by the Metropolitan Police. The report included the results of a public survey which showed: • 57% of those surveyed felt police use of LFR is acceptable; • public support increases to 83% acceptance for LFR to search for serious offenders; • 50% of those surveyed feel that the technology would make them feel safer; *and* • approximately one third raised concerns about the impact on their privacy. The legality of the use of LFR in a public place was also the subject of civil court proceedings in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)* and subsequently in the Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 which concluded:* *".....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."* And 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 dependent on the will of those who apply it, rather than on the law itself".*

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

• Data subjects	• Legal	• Partner agencies
• Union representatives	• OPCC	• Data processors
• Information Assurance	• PSD / Counter Corruption	

Who	When	How	Outcome

South Wales Police Live Facial Recognition Team	21.3.24	Via Teams	Best practice discussed around NWP's use of SWP technology and deployment
South Wales Police visit to Holyhead Port	4.4.24	In person	Discussed proposals for a deployment, its practicality and use. Agreed provisionally to the use, and that our plans are in line with best practise
Greg George – Diversity lead	8.4.24	Via Teams	Equality Impact Assessment screening tool completed. Agreement that NWP's use of LFR will be taken to the NWP Ethics Committee for full review, post initial deployment.
NWP LFR task and finish group	9.4.24	Via Teams	Discussion with DPO, Legal, Diversity lead, Port police team and Comms around NWP's delivery of LFR capability.

Step 4: ASSESSING NECESSITY AND PROPORTIONALITY
In this section you must demonstrate why the processing is necessary[?] and proportionate[?], providing evidence to support your assessment.
4.1 How will processing the personal data help to achieve your purpose? Clearly state your objective and provide evidence for why the proposal is necessary. The evidence can consist of facts, statistics, reports etc.
NWP will use LFR in an overt capacity to help us protect the public. NWP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool. LFR helps NWP use its resources more efficiently. NWP considers that LFR is better than humans at recognising persons from a large dataset (generally hundreds to low thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to NWP. The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies. (It is acknowledged that

considerations regarding data protection should not be considered as an absolute barrier to information sharing).

Locations for the deployment of LFR will be kept under strict review, with LFR being deployed into areas where it has the greatest potential to assist NWP in discharging its operational duties.

The decision to deploy LFR will always be supported by a rationale that explains why a location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other NWP LFR Documents.

Given that LFR requires a member of police personnel to review every Alert in real-time for a decision as to whether any further action is required, NWP will always deploy LFR in a way that is operationally effective and allows NWP to act on any Alerts as they are generated. LFR will not be used indiscriminately.

Images that may be deemed appropriate for inclusion within an LFR Watchlist include 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 restrictions that would be breached if they were at the location at the time of the deployment; *and/or*

d) missing persons graded at medium or high risk; and/or

e) presenting a risk of harm to themselves or others; *and/or*

f) victims of an offence, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progression of an investigation, or is otherwise a close associate of an individual who would fall within criteria (a) – (e).

A rationale for each is as follows:

a - Wanted by the courts. This term includes those with outstanding arrest warrants or who are otherwise required by the courts. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general.

b - Suspected of having committed, be about to, or to be committing an offence. This encapsulates persons who are wanted by the police pre-charge in relation to them being suspects for an offence. This falls within the common law purpose of the police to investigate, prevent and detect crime.

c – Bail conditions, court order, or other restrictions that would be breached. This takes into consideration the fact that an assessment has already been made by either the police or the courts to impose conditions, usually for safeguarding or preventative reasons, and that it is again within the common law purpose of the police to prevent and detect any such breaches.

d – Missing persons graded at medium or high risk. MFH cases of medium or high risk mean that the subject is at risk of danger to themselves or others, with high risk reserved for cases of an immediate risk with substantial grounds for believing that the subject is in danger, or that the public is in danger. Both categories engage the police's responsibilities under Article 2 of the Human Rights Act, and the use of LFR to locate the person is a proportionate way of doing so given the risk and the obligations under Article 2.

e - Presenting a risk of harm. Mitigating the risk of harm to themselves or to others will need to have a legal basis for action under a policing common law power. 'Harm' can include a risk of harm arising in relation to a person's welfare and/or a financial harm, perhaps because of fraud or other dishonesty. It can also include 'harm' in the context of posing a risk to national security.

The risk of harm will be informed by the intelligence case and/or the considerations set out in the applicable LFR deployment application form. This will need to inform the AO as to how the individual or group of individuals present(s) a risk of harm to themselves or to others and:

a) how using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*

b) why the significance of the harm identified means it is **necessary** for the police to take action in order to manage the risk.

The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and

b) the importance of locating the person or people sought with reference to the threat, harm, and risk which the addition to the Watchlist addresses.

c) whether the significance of the threat, harm and risk identified which inclusion on the watchlist would address, outweighs any expectations of privacy.

f - victims of an offence, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progression of an investigation or is otherwise a close associate of an individual who falls under one of the previous headings. This criterion includes a victim, a person who the police have reasonable grounds to suspect would have information of importance and relevance to the progress of an investigation, or a close associate (partner etc.) of an

individual, and that individual who would themselves fall within one of the aforementioned categories that may be deemed appropriate for inclusion within an LFR Watchlist.

The threshold for any Watchlist inclusion is high and the use of this category will be by exception with regard to strict criteria. The necessity for inclusion must be based on a specific intelligence case with the need for the inclusion on a Watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to able to demonstrate to the AO's satisfaction:

A) why the inclusion of each victim, person reasonably suspected of having information, or close associate is **necessary** to help locate the person who is wanted by the courts and/or the police; *and/or*

B) why locating each victim, person reasonably suspected of having information, or close associate is **necessary** to advance the policing investigation; *and/or*

C) why locating each victim, person reasonably suspected of having information, or close associate is **necessary** to ensure their safety and/or the safety of others

The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and

b) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses.

c) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any inclusion on the Watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others.

4.2 Ensuring data minimisation

- Describe whether any less intrusive options would achieve the same goal.
- Could existing processes or techniques be used instead of new intrusive measures?
- Clearly outline why the processing is proportionate.

It is NWP's position that if a decision is made by the authorising officer to deploy LFR technology, then this follows a clearly defined rationale as to why that specific deployment is necessary, proportionate and justifiable, and that there are not any less intrusive options available which would achieve the same goal.

Examples of less intrusive options could be:

- An authorisation granted under Section 60 of the Criminal Justice and Public Order Act 1994, to provide a power to stop and search persons under certain circumstances. This would require personal interaction with a number of people by police officers. The use of LFR allows targeted interactions from a with-cause basis.
- In a port environment, stopping every person passing through to check their passport / ID and travel documents, and then checking this against police databases. This would require every person passing police officers to be stopped, it would significantly delay the public's process and progress through the port and lead to significant delays and disruption. This is avoided by the use of LFR which again allows for targeted engagements.
- The search for missing people by entering houses of associates / relatives. This creates intrusion into their personal life, which would be avoided by the use of LFR.
- The search for wanted people by entering houses of associates / relatives. This creates intrusion into their personal life, which would be avoided by the use of LFR.
- The use of targeted interception of communication data to locate wanted offenders. This creates layers of intrusion, and again can be avoided by the use of LFR deployed to a location where we believe that persons may be present.

4.3 Lawful basis

To process personal data you must have a lawful basis. Please select a lawful basis from the drop down lists (where appropriate). Guidance on lawful processing can be located on the ICO website.

Lawful Basis for Law Enforcement Data[?] *(If applicable)*: Necessary for a law enforcement purpose
Lawful Basis for General Data[?] *(If applicable)*: Choose an item.

4.3.1 Lawful basis for special category data

If any of the special categories of data are being processed, you need to specify an additional lawful basis for processing this data. Please complete the section relevant to your proposal.

Law Enforcement Data[?] *(If applicable)***:**
It is based on law (please tick to confirm) ☒ Common Law Policing Powers.
And
It is necessary for one of the following conditions (select from the list): Justice

General Data[?] *(If applicable)***:**
It is necessary for one of the following conditions (select from the list): Choose an item.
Or
It is in the substantial public interest and for the following purpose: Choose an item.

4.4 Describing compliance

You should include relevant details of how you will ensure compliance:

Data quality How do you intend to ensure and maintain good data quality?	Members of the public – processing will be real time. Watchlist – checks must be made to ensure that the images uploaded to the watchlist are the most recent and up-to-date image of the individual. Watchlists uploaded to the LFR application will not be more than 24 hours old to provide increased assurance that those on the list remain of interest to

	NWP. Technical measures are also in place to cross reference data to the PNC to verify that individuals are still of interest prior to the encrypted transfer to the LFR application. A new Watchlist is generated for every LFR Deployment. The application assesses image quality and suitability for comparison allowing NWP personnel to consider and manage the risk of poor-quality images which are likely to generate False Alerts.
Transparency How do you intend to provide privacy information to people?	Information around NWP's use of LFR will be contained on the NWP website. Engagement teams will hand out leaflets to members of the public during deployments with a link to the website. Signage will be in place at each deployment location advising the public of the use of LFR. It is anticipated that no person will enter the zone of recognition without their knowledge.
Data subject rights What mechanisms will you put in place to ensure data can be searched, extracted, printed, deleted, rectified or restricted?	Following each LFR deployment, the Silver Commander must ensure that a post-deployment evaluation is completed which is updated in the Deployment Record. The evaluation process must capture an assessment of the operational effectiveness of the LFR deployment. This evaluation should be both qualitative and quantitative in nature. The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the deployment and what opportunities exist to improve them for future use, and how learning will be shared. The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (<u>including</u> what methods were used to obtain them):- (a) total number of individuals <u>and</u> the total number of images included in the Watchlist (there may be multiple images of some individuals); and (b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR application was able to generate a template from them); and

	(c) total number of LFR application-generated Alerts; and (d) total number of Alerts that do not result in an engagement; and (e) total number of Alerts where a decision was taken to engage an individual; and (f) total number of Alerts that are confirmed as true alert (the individual is who the LFR application suggests are); and (g) total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and (h) total number of correct Alerts that result in an engagement that do not require any further police action; and (i) outcome of each case where police action is instigated following an Alert; and (j) number of people Engaged, where the engagement was not the result of Alert, including the reasons and outcome; and (k) Threshold setting for the deployment. These records will be published on the NWP website post-deployment and will be available to data subjects.
Processors If you are using a data processor, what measures do you take to ensure processor compliance? E.g. a contract, audit, sufficient guarantees.	There will be a data processing agreement in place with SWP.
International transfers Outline how you will safeguard any international transfers.	N/A
Purpose limitation How will you prevent function creep?	The deployment of LFR will be subject to approval and authorisation by an officer of at least the rank of ACC. The authorisation will set out the criteria for compiling the watchlist, along with the justification and proportionality for the deployment.

	The authorisation will also be subject to a cancellation in due course. The deployment will also be overseen by a Silver commander and a Bronze, ground assigned commander, who will oversee the use, ensure the watchlist remains current, and safeguard against function creep.

What to do next

You will need to detail all data protection risks within steps 5 and 6 (on the following pages), including the impact on individuals (and their privacy) as well as risks to the organisation. To assist, these sections focus on specific data protection principles and privacy concerns. The risk matrix at the end of the document also provides support in determining the risk rating.

Step 5: RISK ASSESSMENT		
Identify and assess risks ✓ Detail **all** data protection risks, privacy and the rights and freedoms of individuals. ✓ Consider the impact? on individuals and any harm or damage that might be caused. ✓ Where risks are identified, you must take steps to integrate solutions into the project and this must be recorded. ? Examples of risk factors are provided as a starting point. You must ensure that all factors relevant to your proposal are considered. If you run out of space then insert my lines into the table. If you are unable to identify a risk then please state "**No risks identified**".		
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	**Corporate risks include:** • Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations	**Mitigation/solution examples:** • Deciding not to collect certain types of data • Reducing the scope of processing • Reducing retention periods • Taking additional technical security measures • Providing staff with training and guidance to understand the risks • Anonymising or pseudonymising the data • Using different technology • Using an alternative third party processor
5.1 Being fair and lawful		
Data must be processed lawfully, fairly and in a transparent manner? • Have you identified the lawful basis of the project?		

- Do you need to create or amend a privacy notice?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm** *Remote* *Possible* *Probable*	**Severity of impact** *Minimal* *Some* *Serious*	**Initial risk[?]** *High* *Medium* *Low*	**Mitigation/solution** *Describe the mitigation and whether it will be implemented*	**Result** *Is the risk:* *Eliminated* *Reduced* *Accepted*	**Residual risk** *High* *Medium* *Low*
Discrimination	Remote	Serious Harm	Low	The measures taken to reduce system discrimination are included within the force policy on LFR, under the measures for testing equitability. This is based on scientific evidence. NWP is confident that the system is not inherently discriminatory. Our policy and SOP will be publicly available, and we are confident in the ability to demonstrate the system accuracy.	Reduced	Low
Reputational damage / embarrassment	Remote	Serious Harm	Low	The use of LFR complies with best practise, APP, and force policy. LFR has been in use by police	Reduced	Low

				forces for a number of years, and has been subject to numerous reviews, scientific studies and recommendations around its use by relevant bodies. NWP's use of the technology fully complies with this and is subject to a detailed authorisation process for its use, authorised by chief officer level. We are satisfied that the risk of reputational damage to NWP is low. There are always those who may complain about its use, however studies and surveys show that the majority of the public are accepting of this and supportive of its use.		
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	Possible	Some Impact	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	Accepted	Low

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.				justification will be documented prior to any Deployment.		

5.2 Having a specific, explicit and legitimate purpose

The purpose for processing personal data must be specified, explicit and legitimate, and not further processed in a manner that is incompatible with the original purpose for which it was collected.

- Does your project plan cover all of the purposes for processing personal data?
- Are all elements of the processing compatible with the original reason and justification for the processing?

Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	Likelihood of harm	Severity of impact	Initial risk?	Mitigation/solution	Result	Residual risk
No risk identified	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.3 Recording adequate, relevant data and not being excessive

Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed

- Is the quality of the information adequate for the purposes it is used?
- Are measures in place to ensure that data is limited to that which is needed to fulfill the aim of the processing?
- Which personal data could you not use, without compromising the needs of the project?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
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 data may be excessive resulting in regulatory action.	Possible	Serious Harm	High	The assessments prior to a Deployment will consider and document why less intrusive methods are not appropriate and justifying the use of LFR based on intelligence.	Reduced	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.	Possible	Some Impact	Medium	The Watchlist can be re-engineered. This can now be achieved via Niche RMS 'back-end' database by recording the nominal number of an individual extracted into a Watchlist for any given date	Eliminated	Low
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	Remote	Serious Harm	Low	The technology has been trialled and tested by SWP. NWP have adopted the best practise process and procedures which have been developed and tested by SWP.	Reduced	Low

Possible Matches resulting in potential damage and distress or threat risk and harm to others.				NEC algorithms have also been evaluated by the National Physical Laboratory (NPL), NIST and the Department of Homeland Security and NWP pays regard to these findings. 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 present at all Deployments. All relevant information is logged for audit purposes. Logs are kept by the Gold, Silver and LFR Operator and LFR Engagement Officer. NWP 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 SWP's 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.		

5.4 Ensuring data is accurate & timely

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

- If you are procuring new software, does it have controls in place to assist accurate data recording?
- Does the new software allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- Do you have processes in place to keep data up to date?

Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	Likelihood of harm	Severity of impact	Initial risk?	Mitigation/solution	Result	Residual risk
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 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	Remote	Some Impact	Low	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 Possible Matches without manual intervention to reduce any damage and distress.	Reduced	Low

potentially cause unwarranted and unjustified damage and distress to individuals.						
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.5 Retention of personal data

Personal data must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data.

- What are the risks associated with how long data is retained and how they might be mitigated?
- Has a review, retention and disposal (RRD) policy been established?
- You may wish to consult the Force Records Manager.

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
Personal data used to compile the watchlist is produced from NICHE RMS records. This is retained in line with MOPI records. No specific risks for this process.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
Data obtained during the deployment is subject to immediate deletion if there is	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

not a match. No risks regarding retention.						
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.6 Keeping personal data secure

Personal data must be processed in a manner that ensures appropriate security[?] of the personal data, using appropriate technical or organisational measures.

- What technical and organisational measures are in place to ensure that the date is protected to an adequate level?
- What training on data protection and/or information sharing has been undertaken by relevant staff?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
Access to data held by the LFR system must be secure.	Remote	Serious Harm	Low	Two types of access will be available to the application – 'user' and 'administrator' access levels Operating staff will all be vetted and cleared to at least MV/SC level. Role- based access controls	Accepted	Low

				Access is only granted to users following completion of training. The application has an in built and robust audit file log CSV file (hashed). Each LFR Operator will be given a username and password which they will be forced to change on initial use of the application ('Active Directory' strength of eight characters to include upper and lower case as well as being alpha numeric. Local network passwords are security protected. The application is non-networked and non-configured to extend to the cellular network – essentially an additional geographical protection. The application is non-networked and non-configured to extend to the cellular network – essentially		

				an additional geographical protection. The LFR application is 'closed' and not connected to other NWP or SWP systems or the internet. As a contingency against the technology failing and requiring the LFR Operator to wipe and reset it the encrypted USB memory stick is retained with the LRF Operator under the end of the Deployment meaning that they are able to reimport the watchlist to the rebooted LFR application enabling the Deployment to continue. The use of LFR technologies is governed by a number of codes of practice including those applying to the police such as PACE. In particular the use of LFR is covered in the twelve principles		

				laid down in the Surveillance Camera Code of Practice, to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras applies to their use by the police and other authorities. Images are transferred onto the LFR application via a USB using an AES-CBC 256-bit full disk hardware encryption engine that is further protected bypass number access. Access to the USB stick containing the Watchlist is limited to those with a need to use it.		
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.7 Complying with data protection rights

Data Protection legislation gives data subjects various rights. Limiting or restricting any of these rights is likely to be a significant impact so the justification for any restriction, as well as mitigations, must be fully outlined.

- Consider each of the rights listed below and assess whether data subjects would be able to fully exercise these rights.
- For example: If an individual makes a Subject Access request, will you be able to easily identify, retrieve and extract the data to provide to the Information Assurance /Subject Access team?

Right to fair processing information[?]
Right of access (subject access)[?]
Right to rectification[?]
Right to erase or restrict processing[?]
Rights regarding automated decision making and profiling[?]
Right to object[?]

Describe the source of risk and the nature of potential impact on individuals[?] **and the organisation**[?]**.**	**Likelihood of harm**	**Severity of impact**	**Initial risk**[?]	**Mitigation/solution**	**Result**	**Residual risk**
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.	Possible	Serious Harm	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	Eliminated	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.8 External data sharing and international transfers						
Your processing may involve the sharing of personal data with 3rd party individuals, organisations or agencies. • What contracts, information sharing agreements or memorandums of understanding are in place? • What assessments have been made of the 3rd parties to ensure adequate provisions for the technical and organisational security of personal data? • Has the organisation specifically asked suppliers to undertake a DPIA? • If you will be making transfers, how will you ensure that the data is adequately protected? (especially if outside of the EU) • Will we share data with a third party processor based outside the EU?						
Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	**Likelihood of harm**	**Severity of impact**	**Initial risk?**	**Mitigation/solution**	**Result**	**Residual risk**
North Wales Police will be sharing data with South Wales Police for the NWP generated watchlist to be uploaded to LFR systems. **Without appropriate data sharing agreements the force could be subject to civil action around data protection**	Remote	Some Impact	Medium	A data sharing agreement will be in place with South Wales Police to cover any deployments.	Eliminated	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.9 Human rights considerations

The European Convention on Human Rights sets out numerous rights and freedoms. Limiting or restricting any of these rights is likely to be a significant impact and result in a residual high risk. The justification for any restriction, as well as mitigations, must be fully outlined.

- If your actions will interfere with any of the rights listed below then you must clearly outline why it is necessary and proportionate.
- You must first consider: **Article 8: Right to privacy** – Will the proposal adversely impact an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications?

The Rights are:

Article 2: Right to life
Article 3: Prohibition of torture
Article 4: Prohibition of slavery or forced labour
Article 5: Right to liberty and security
Article 6: Right to a fair trial
Article 7: Right to no punishment without law
Article 8: Right to respect for private and family life without law
Article 9: Right to freedom of thought, conscience & religion
Article 10: Right to free expression
Article 11: Right to freedom of assembly and association
Article 12: Right to marry
Article 14: Right to freedom from discrimination

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
LFR impacts on Article 8. Consideration must be given to this in all plans and authorisations.	Probable	Serious Harm	Low	NWP use of LFR must be in compliance with the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and in particular has the potential to impact upon an	Reduced	Low

				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.' 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. It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom* 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". The High Court and Court of Appeal Bridges cases considered Article 8, specifically in the context of LFR technology and confirmed that Article 8 is engaged in so far as someone passes through the Zone of Recognition and in so far as someone is placed on a LFR Watchlist for a Deployment. Depending on the nature of the deployment, the 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 expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. Authorising Officers should contact NWP Legal should they		

				consider a proposed deployment may have a wider human rights point to consider. A legal mandate has been created and overviewed by NWP's legal department. This details the legitimate, necessary and proportionate aims of a LFR deployment. The intrusion of rights under the Human Rights Act are also required to be considered by the authorising officer prior to any deployment, and they are detailed in a form which will be saved and auditable.		
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.10 Additional risk factors

Describe any further risks, ensuring that any risks not already identified are included.

Additional risks may for example include:

- Internal data sharing - With which parts of the organisation is the information shared, what information is shared and for what purpose?

- If you are processing special categories of data then what risks have you identified?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
A.I risks are present, and if not used properly then this could have a detrimental impact on force reputation	Possible	Some Impact	Medium	Full policy, standard operating procedure, legal mandate are present and auditable. These conform to best practice with regard to APP. In addition, A.I risks are included on the force risk register and are subject to senior leader review.	Reduced	Medium
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

Step 6: LAW ENFORCEMENT RISKS

This section is only applicable to proposals involving law enforcement data. **Move to Section 7 if solely processing general data.**

6.1 Data logging requirements

Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

- If the data is processed electronically, will a log be retained of the following actions?

• **Collection** • **Disclosure** • **Erasure** • **Alteration** • **Combination** • **Consultation**	☒ **Yes** ☐ **No (risk must be recorded)**

Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	**Likelihood of harm**	**Severity of impact**	**Initial risk?**	**Mitigation/solution**	**Result**	**Residual risk**
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

6.2 Data categorisation requirements

When processing data for law enforcement purposes, you must provide where relevant and as far as possible a clear distinction between categories of data subject.

- Will there be a clear distinction between different categories of personal data subjects, for example subjects who are:

• **Suspected of having committed, or are about to commit, a criminal offence** • **Convicted of a criminal offence,** • **Victims of a criminal offence,** • **Witnesses to a criminal offence.**	☒ **Yes** ☐ **No (risk must be recorded)**

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

In Step 7, please indicate where mitigation/solutions and residual risks have been approved by the Head of Department/Information Asset Owner.

Step 7: OUTCOME AND REVIEW		
Item	**Name/Date**	**Notes**
Solutions approved by:		Integrate actions back into the project plan, with date and responsibility for completion.
Residual risks approved by[?]:		The Head of Department/Information Asset Owner must approve all residual risks.
If any residual risks remain High		
Date forwarded to DPO:		If any residual risks remain High, please forward initially to the Data Protection Officer (DPO) for their advice.
Summary of DPO advice: Click here to enter text.		
Date forwarded to CIO/SIRO:		Any residual risks remaining High must be referred to Chief Information Officer (CIO)/Senior Information Risk Officer (SIRO) for the risk to be accepted prior to referral to ICO.
High risk(s) accepted by:	Name: SIRO/CIO *(please delete as appropriate)* Date:	
Date forward to ICO		If accepting any residual high risk, the ICO must also be consulted before commencing processing.
Review		
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live.		
Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged. Please also include; • who will be responsible for reviewing the processing;		

DPIA Nov 2018 (V 1.0)

- the frequency of the review; and
- the date of the next review.

Click here to enter text.

How to identify and assess risks (Risk Matrix) *(Click the triangle to expand)*

You will need to consider the potential impact on individuals and any harm or damage that might be caused by the processing – whether physical, emotional or material. In particular, look at whether the processing could possibly contribute to:

- Inability to access rights or access service or opportunities;
- Loss of control over the use of personal data;
- Discrimination;
- Identity theft, fraud or financial loss;
- Reputational damage;
- Physical harm;
- Loss of confidentiality;
- Re-identification of pseudonymised data; or
- Any other significant economic or social disadvantage.

You will also need to include an assessment of the security risks and the potential impact of a breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is high, you will need to make an 'objective assessment' considering both the likelihood of harm and severity of impact. The matrix below assists to determine the initial risk.

DPIA Nov 2018 (V 1.0)

Risk Matrix:

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some Impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Possible	Probable
		Likelihood of harm		

DPIA Nov 2018 (V 1.0)