DPIA Ref:
Police Force:

Data Protection Impact Assessment (DPIA)

You should start to fill out this template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated into your project plan. Please provide as much details as possible, avoiding jargon or acronyms where possible

Controller details

Name of Force	South Wales Police (SWP) Gwent Police (GWP)
Subject/Title of DPIA	Retrospective Facial Recognition (RFR)
Name of Data Protection Officer	Louise Voisey

Project Name	Retrospective Facial Recognition
Responsible Owner	Inspector Ben Gwyer
Business Area/Department	Digital Services Division
Proposed implementation date	21.11.2022
Version No.	0.3

It is recommended that you refer to the DPIA guidance and process documents (hyperlink) to assist in the completion of these sections.

Terms & Definitions: Capitalised terms used within the RFR DPIA shall have the meaning given to them in section 3 of the RFR Policy document and Annex B of the DPIA unless otherwise defined.

Step 1: Project Aims and Processing

Explain what the project or processing aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents

Retrospective Facial Recognition (RFR) is recognised as 'post event' use of facial recognition technology, which compares still images of faces of unknown Subjects against a Reference Image Database in order to identify them.

The RFR process utilises the Facial Recognition Technology (FRT) System by ingesting a Probe Image or video clip containing the unknown Subject. A Biometric Template is created for the unknown Subject and compared against a lawfully held database of images (Reference Image Database) held by South Wales Police, at present this is roughly 800,000 images. Up to 200 results are returned from this comparison for review by a trained RFR Operator. The results generate a Similarity Score with which the FRT System ranks the Possible Matches.

The results are reviewed by a trained RFR Operator who assesses the quality of the Possible Match, records the outcome and if the match is deemed to be suitable, the results are referred to the Investigating Officer for progression of the investigation. The FRT System suggests Possible Matches based upon the similarity to the compared Biometric Templates. The FRT System does not replace the role of a human in reviewing and quality assuring the outcomes

When to use RFR?

To Identify:

1. Individuals suspected of criminality and who are wanted by the courts and police.
2. Individuals who may pose a risk to themselves and others.
3. Individuals who may be vulnerable.
4. To effectively demonstrate the technology to the public and wider community to aid understanding, reassurance and to provide greater transparency.

Personal data: Outline what categories or personal data will be processed and explain why each is necessary to achieve the project aims. *E.g. names, addresses, DoBs, criminal records, 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 RFR. This may include but not limited to the name, date of birth and address of an individual. These details will 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 Reference Image Database will include a Niche nominal number.

Special Category data: please select all applicable categories below which will be processed
☒ Race ☒ Ethnic origin ☐ Political opinions ☐ Sex life ☐ Religion ☐ Philosophical beliefs ☐ Trade union membership ☐ Genetic Data ☒ Biometric Data ☐ Sexual orientation ☐ Health ☐ None 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: a. eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act

b. advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it
c. foster good relations between persons who share a relevant protected characteristic and persons who do not share it.'

It should be noted that processing personal information as part of an FRT Equitability Evaluation will be detailed in a separate DPIA.

Data Subjects: What categories of data subject are involved?

x Persons suspected of having committed or being about to commit a criminal offence
x Persons convicted of a criminal offence
x Persons who are or may be victims of a criminal offence
x Children or vulnerable individuals
x Police officers or staff (current and former)

If other, then please provide further details below:

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 identify and/or safeguard these individuals.

Step 2: Describe the processing

Describe the nature of the processing: How will you collect use, store and delete data? What is the source of the data? Will you be sharing with anyone? Consider the end to end process and provide these details for each step of the process.

If possible, please include/attach a flow diagram or infographic.

What types of processing identified as high risk are involved?

Will you be collecting new information about individuals?

The technical operation of RFR comprises the following six stages:

(1) Compiling/using an existing database of images. RFR requires a database of existing facial images (referred to in this case as a Reference Image Database) against which to compare facial images and the biometrics contained in them. For such images to be used for RFR, they are processed so that the "facial features"

associated with their Subjects are extracted and expressed as numerical values.

(2) Facial image acquisition. Probe Images can be obtained from a variety of sources to include but not limited to; CCTV, Body Worn Video, mobile phone footage, social media images.

(3) Face detection. Once a Probe Image is supplied to the FRT System, the software
(a) detects human faces and then
(b) isolates individual faces.

(4) Feature extraction. Taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face, the resulting Biometric Template being unique to that image.

(5) Face comparison. The FRT System compares the extracted facial features with those contained in the facial images held on the Reference Image Database.

(6) Matching. When facial features from two images are compared, the FRT System generates a Similarity Score.

Reference Image Database

The Reference Image Database includes lawfully held custody images from SWP/GWP Niche Record Manage System (RMS). Reasonable steps have been taken to ensure that the image is of a person intended for inclusion in the Refence Image Database.

Niche RMS is a collaborative crime recording system hosted by SWP but also utilised by GWP with all custody images being accessible across both forces.

Every custody image relating to an individual will be imported into the FRT System, this is necessary because often the Matched image may not be from the most recent custody image of an individual.

The Candidate Images within the FRT System are retained in line with Management of Police Information (MOPI) retention periods which mirror the original custody image within Niche RMS.

Given the potential for System Factors relating to age, specific regard needs to be had to the importance of identifying those aged under-18 on a risk-based approach in line with the SWP/GWP Documents, with a particular focus on ensuring the necessity case is fully made out.

If RFR is to be used to identify person aged under 13-years-old, specific regard should be had to anticipate FRT System performance issues. Specific advice will be sought from the Identification (ID) Manager.

Describe the scope of the processing: How much data will you be collecting and using? How often? How long will you keep it? How many individuals' data will be involved? What geographical area does it cover?
The Reference Image Database currently has circa 800k Candidate Images, this will increase on an average rate of 100 Candidate Images per 24 hour period. **Retention and Erasure** **Particular to the FRT System** • Image of the Subject ('Probe Image') - MOPI retention of personal information • Biometric Template of Probe Image - immediately deleted in the FRT system. • Reference Image Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS **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
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have over the processing of their data? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns or challenges over this type of processing or security flaws?

Is the processing new in any way? Are there any current issues of public concern that you should factor in?
Members of the public The use of RFR is subject to a series of RFR Documents that are available to the public on the South Wales Police/ Gwent Police website. Any member of the public who is subject to RFR use will include: - • Individuals suspected of criminality and who are wanted by the courts and police. • Individuals who may pose a risk to themselves and others. • Individuals who may be vulnerable. **Reference Image Database** Those included in the Reference Image Database will be individuals where a custody image has been lawfully captured and retained. 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. **Children/Vulnerable Groups** It is possible that there will be processing of children or vulnerable groups. Where there is a Possible Match, the RFR Operator will be alerted and further manual checks will be carried out to identify whether that person is on the Reference Image Database. There is no automated decision making in the process. Given the potential for System Factors relating to age, specific regard needs to be had to the importance of locating those aged under-18 on a risk-based approach in line with the SWP/GWP Documents, with a particular focus on ensuring the necessity case is fully made out. If RFR is to be used to locate person aged under 13-years-old, specific regard should be had to anticipate FRT System performance issues. Specific advice must (at this time) be sought from the IDManager.

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 RFR 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.

Safeguards – there are concerns that there are insufficient safeguards around the use of RFR.

Function creep – there are concerns that RFR will be used to monitor movements and action of the public beyond the scope of targeted use.

Retention – there are concerns that all data utilised by RFR will be kept as intelligence.

Bias – there are concerns that the software algorithm may contain inherent bias with regard to the protected characteristics of race, age and gender. The National Physical Laboratory: *'Facial Recognition Technology In Law Enforcement Equitability Study', referred to as the NPL Equitability Study,* considers this area of further detail:

frt-equitability-study_mar2023.pdf (science.police.uk)

The human failsafe of an officer (RFR Operator) checking the Probe 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. SWP and the National Police Chiefs Council (NPCC) are keen to continue to engage with the Home Office with regards legislative improvements.

Describe the purposes of the processing: what do you want to achieve through the processing of this data? Will there be any impact on the individuals whose data is being processed?
What are the benefits of the processing – for you, and more broadly?

RFR 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 RFR may assist Forces achieve their policing purposes:

a. supporting the identification and arrest of people wanted for criminal offences

b. 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)

In an austere climate, the challenges presented in identifying 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.

Step 3: Consultation

Consider how to identify and consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

A number of stakeholders have been engaged from the outset of this project initially by South Wales Police to ensure legitimacy and transparency in terms of privacy and its potential impact upon communities. The following have already been consulted, but the list remains organic along with the DPIA itself as Deployments mature and develop:

1. Information Commissioner's Office – Advice and guidance was received from the ICO. Opinion on Deployment of Live Facial recognition in public places and interested party in *(on the application of Edward Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058*.

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 our 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 image.

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 – Professional discussion over Deployment of an LFR APP

11. Police Digital Service – Professional discussions over system developments against a desired national rollout picture of the future.

12. The National Physical 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. This study is referred to as the NPL Equitability study.

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 dependant on the will of those who apply it, rather than on the law itself".

16. Publication consultation sessions have been completed at various locations across South Wales Police force area over a four-year period. These have culminated in workshops delivered at SWP HQ. There has also been public consultation during each Deployment of the technology. Public consultation will continue at appropriate events where it is practicable to do so. This has been deemed particularly successful when LFR is deployed where an opportunity exists to demonstrate the technology.

17. Participation by Chief Constable Jeremy Vaughan in the SCC/BC event 'Is there a legitimate role for facial recognition in policing and law enforcement' at the London School of Economics on the 14th June 2022. Attendance included academics, technologists, representation from civil libertarian groups and broader society.

18. Public Perception Surveys – South Wales Police 2022: More recent studies of the technology have been conducted by South Wales Police as 'Show and Tell' style events. The engagement events have taken place in a variety of locations over the Summer of 2022 resulting in 155 responses.

In considering the results of this study, the following headlines are apparent:

- 88.4% of individuals were not concerned by SWP utilising Live Facial recognition in comparison 10.3% who had concerns. The concerns expressed related to data protection issues and general trust in the Police
- 76.8% of respondents considered that SWP use of LFR would lead to little or no impact upon them going about their daily business in comparison to 7.7% who considered it would have a large or significant impact upon them going about their daily business
- 79.4% of respondents stated that they would not change their plans to attend a location where they knew SWP were utilising live facial recognition compared to 6.5% who said they would.

Step 4: Lawfulness, Necessity and Proportionality

Please provide information on following requirements or seek advice from the DPIA adviser or DPO:		
Is the processing for Law Enforcement Purposes or general processing? ICO Guidance on Law Enforcement Processing and General Processing	Both	
Legal power to carry out processing e.g. statute, common law, court order etc. *(please provide details)*	Common law – policing purpose and law enforcement purpose. Police and Criminal Evidence Act (PACE) 1984 The RFR Legal Mandate provides detailed analysis relating to article 8 of the Human Rights Act 1998 and other relevant legal considerations.	
Lawful basis for processing *(please select the appropriate conditions. If different conditions apply to different stages of the processing please provide further details)* *General Processing (GDPR):* *Please select one condition for processing personal data. If processing special category data please select a further condition.* *ICO Guide to GDPR - Lawful Conditions for processing* *Law Enforcement Processing:*	**General: Personal data** ☐ Consent ☐ Contract ☐ Vital Interests ☐ Legal Obligation X **Public Task** ☐ Legitimate Interests	**General: Special category data** Explicit Consent ☐ Obligations & rights in employment, social security & social protection law ☐ Vital interests ☐ Members of former members of a

Please select one condition for processing personal data only. *If sensitive processing takes place please select a further condition.* *ICO Guide to Law Enforcement Conditions*		not for profit body ☐ Data has been made manifestly public by the data subject ☐ Legal claims X Substantial public interest ☐ Health ☐ Public interest in Public Health ☐ Archiving X Historical research It is considered that the identified processing of sensitive information is strictly necessary and there is a pressing social need which cannot reasonable be achieved through less intrusive means. The pressing social need seems to concern the weight and importance of the aims pursued. Over the life of the project and at any one time SWP / GWP is seeking to arrest (where the necessity test is made out) 350 individuals wanted on warrant and 350 individuals suspected of criminality. In order to best serve

		the community and in particular the victims, realising swift justice is a considerable aim. Likewise for RFR, there are other more traditional ways of identifying persons suspected of committing a criminal offence. An image of the suspect could be shared with colleagues, circulated on social and national media. It is probably prudent at this stage to point out like other Police forces across the UK, SWP/GWP front line officers are generally very young in service, these officers would normally deal with the majority of crime where a suspect has been identified. The ability of young in service officers to recognise historical offenders may be limited, which would naturally result in suspect images being circulated more wider than ever before. It is believed that the use of RFR is far less intrusive in identifying a suspect than employing traditional methods as it doesn't disclose

		the image of an individual to the wider community as being suspected of involvement in crime, or in particular, crime of a particular nature that might have significantly wider impact such as sexual offences.
	Law Enforcement: Personal data ☐ Consent X **Processing is necessary for the performance of a task carried out for that purpose by a competent authority.**	**Law Enforcement: Sensitive processing** ☐ Consent X **Processing is strictly necessary for the law enforcement purpose; and** **X Statutory etc purposes** **X Administration of justice** **X Protecting vital interests** **X Safeguarding of children and individuals at risk** ☐ Personal data already in the public domain ☐ Legal claims ☐ Judicial Acts
DPA2018 (to be completed where special category data (part 2) or sensitive processing (Part 3) is being carried out	Schedule 8 (Part 3) para 1 – Statutory purposes Schedule 8 (Part 3) para 2 – Administration of Justice Schedule 8 (Part 3) para 3 – Protecting the individual's vital interests Schedule 8 (Part 3) para 4 – Safeguarding of children and individuals at risk Schedule 8 (Part 3) para 8 – Preventing fraud Article 9 (Part 2) para 2a – Explicit consent	

	Article 9 (Part 2) para 2g – Substantial public interest ○ Part 2 Schedule 1 para 6 Statutory ○ Part 2 Schedule 1 para 18 Safeguarding of children or individuals at risk
Privacy Information – what information will you provide to the individuals whose data is being processed, how will this information be provided and at what stage of the processing activity. If no privacy information is to be provided, please provide the reason for this.	A communications strategy is in place for the use of RFR. RFR Documents are available on the SWP Website. Any person who requires further information relating to RFR should be provided with contact information for the FRT team. An overview of documents available to the public is at Annex A
Will the personal data collected be used for any other purposes? (*Please provide details)*	No.
Will the processing include mechanism to facilitate the exercise of individual rights *(please select which rights can be exercised)*	Right to be informed – members of the public will be informed regards the extent of RFR use via the available RFR Documents. Right to rectification – individuals will be able to challenge the processing where a Possible Match has been identified by RFR and the RFR Operator. Right to erasure – a request can be submitted where a Match has been made and individuals are challenging the outcome. Right to data portability – not applicable Right to object – not applicable under Part 3 DPA 2018. SWP / GWP will assess any right to object requests it receives on a case-by-case basis if a request is received and the

	processing in question does fall under Part 2 of the DPA 2018. Right to object to automated decision-making including processing – no automated decision making will be taking place without any human involvement. All decisions will have manual intervention.
How will you ensure that the data being processed is accurate and up-to-date? Accuracy Will the processing allow you to erase or rectify inaccurate data without delay?	Members of the public – processing will be Probe Images obtained for a policing purpose. Reference Image Database – checks must be made to ensure that the images uploaded to the Reference Image Database are of the individual. The FRT System assesses image quality and suitability for comparison allowing SWP personnel to consider and manage the risk of poor-quality images. As part of the Force procurement process, due diligence must be given to expected algorithm performance (or accuracy). The National Institute of Standards & Technology (NIST) regularly undertake large scale Facial Recognition system tests. While these provide a good starting point, given algorithm-specific variation, it is incumbent upon the system owner to know their algorithm. While publicly available test data from NIST can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data sets. To enhance the ongoing internal understanding of algorithm and software performance SWP has commissioned an independent academic evaluation (subject to separate DPIA) to be completed by the National Physics Laboratory (NPL). This will include an understanding equitability for age, gender and ethnic background. The NPL Equitability Study has assisted in measuring overall accuracy and testing has

	shown that RFR 100% true positive identification rate across all demographic cohorts, with no detectable bias in any of the demographic cohorts SWP/GWP currently use the M40 algorithm supplied by NEC, this is utilised with NEC's Neoface software. The ICO has provided helpful guidance on their expectations for statistical accuracy in that it "does not mean that [the LFR] application needs to be 100% statistically accurate to comply with the accuracy principle". However SWP/GWP gives due regard to the opinion that the frequency of monitoring the algorithm should be proportionate to the to the impact of an incorrect output on an individual therefore SWP/GWP provides for an ongoing evaluation basis. The SWP/GWP supplier has also been held in high regard by the NIST in its 2018 evaluation of over 200 algorithms. SWP/GWP personnel will take all reasonable steps to ensure that each image on the Reference Image Database does actually pertain to the intended person. No action will be taken against an individual without human consideration of a valid match.
Does the processing require you to keep the information in an identifiable form? *(If yes, please provide reasons for this)* Could you pseudonymise or anonymise the data to achieve your aim?	The only information which is retained will need to be identifiable so that the policing purpose/law enforcement purpose can be fulfilled. Any retention will be in accordance with the DPA2018 and theMoPI. Technical systems and standard operating procedures help ensure that data is properly retained or deleted. Processing mechanisms, RFR policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes

	The Candidate Images on the Reference Image Database need to be identifiable to the police and cannot be anonymised or pseudonymised to achieve the aim which is to identify the Subject.
How long do you need to retain the personal data? *(Please indicate the framework under which retention is stated)* What mechanisms are in place to review, dispose of, or delete the data when no longer required?	**Biometric Templates** The Biometric Templates of the Subject are immediately deleted after the RFR search. Biometric Templates of the Candidate Images are retained in line with MOPI retention periods. **Possible Matches** The RFR Operator will typically review the most similar (based on Similarity Score) 200 Possible Matches. RFR Operators may decide to review a greater number of Possible Matches based on the nature of the enquiry, considering underlying threat, risk and harm. **Retention and Erasure** **Particular to the FRT System** • Image of the Subject ('Probe Image') - MOPI retention of personal information • Biometric Template of Probe Image - immediately deleted in the FRT system. • Reference Image Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS **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)

	To ensure parity between the Source System and the FRT System each image is applied a hash value with the values being compared on a daily basis to identify any variance. To that end when an individual successfully applies to SWP/GWP for a non-convicted custody process image to be deleted from Niche RMS the comparison of the hash values would effectively identify the inconsistency between the data sets and an alert email would be sent to the project team to ensure deletion from the FRT System.
What organisational and technical measures will be in place to protect the personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage? How will you monitor the ongoing effectiveness of the security measures? *Note – if you are using data processors what guarantees will you obtain about their ongoing ability to keep the data secure?	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 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 RFR 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 networked within the SWP domain. It is non-configured to extend to the cellular network – essentially an additional geographical protection. The use of RFR is governed by a number of codes of practice including those applying to the police such as PACE 1984. Authority – the governance and authority for RFR is contained in the SWP/GWP RFR Policy. RFR review to the SWP/GWP FRT Board is used to identify lessons for the future and periodic audit provide assurance.

	An **appropriate policy document** outlining the safeguards and controls in place **Assessments** - These include a Community Impact Assessment, an Equality Impact Assessment (or other similar documented record), an overarching DPIA, and the Surveillance Camera Commissioner's (SCC) Self-Assessment. These documents need to be considered by the decision-maker when authorising RFR use to ensure they are sufficient to address the issues arising from the use. The decision maker must involve their DPO in writing the DPIA and in managing the processing of personal data. The decision-maker must ensure that issues have been adequately identified, documented, and mitigated to ensure that RFR use is not only necessary, but also proportionate to the policing purpose. **Operational risk assessment** - A documented assessment of specific operational risks associated with RFR including decisions taken regarding mitigation. The FRT System uses an independent system available within 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 FRT System from Niche RMS via an automated process. Candidate Images will be uploaded into the FRT System on a real time basis. When the Subject has their custody image taken these will be 'seen' by the FRT System and ingested. Currently there is approximately a 5-minute lag between Niche RMS and the FRT System.

	To ensure parity between the image library in Niche RMS and the FRT System each image is applied a hash value with the values being compared on a daily basis to identify any variance. Probe Images will be imported into the FRT System by the RFR Operator. If a Probe Image is of insufficient quality, it will fail to enrol into the FRT System and as such will not be saved in the application. When a Probe Image is compared against the Reference Image Database the Probe Image will be saved into the FRT System and will be retained in line with the MOPI retention categories. A record of the search will be available within the audit log of the FRT System, this will include the Probe Image but the relating Candidate Images are not saved as part of the audit log. The only metadata to accompany the Candidate Image will be the Niche nominal number. The data is held securely on SWP systems accessible to SWP/GWP officers and staff which is fundamentally permission based. Officers leaving SWP/GWP automatically have their account disabled and therefore would no longer have access to the information. SWP/GWP RFR Documents provide for the training of officers and staff involved in RFR . The training helps ensure role specific: 1. familiarity with SWP/GWP RFR Documents; 2. knowledge of RFR use; 3. understanding of the lawful processing of personal data in accordance with the DPA 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 Matches; 6. knowledge of how to configure the FRT System to maximise system performance, and how to minimise impact on others; understanding of the characteristics of the FRT System that affect the likelihood that a Possible Match is reliable.
Will the personal data be held or transferred outside of the UK? *(If yes, please provide details of the location, the environment in which it will be held, reason for transfer and safeguards)*	No.
Will there be an information sharing agreement or contract in place with all parties with whom personal data will be shared? *Please provide details)*	Information will only be shared where necessary for a policing purpose on a case by case basis therefore no agreement is necessary. A contract will be in place with the algorithm supplier The supplier does not have routine access to the software and algorithm supplied to SWP/GWP and do not act as a data processor for the purposes of this DPIA.

Step 5: Identify and assess privacy & compliance risks

No.	Identify risk – Cause, event, effect	Likelihood	Impact	Overall risk
		L,M,H	L,M,H	L,M,H
1	Person identified by RFR wishes to have their data removed from the FRT System.	L	M	M
2	Use of the FRT System generates an incorrect Match.	M	M	M
3	As a result of the scope of RFR use there is a risk that fair processing information may not be 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.	M	M	M
4	Unlawful arrest as a result of an RFR Match	M	M	M
5	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 leading to potential legal challenge, financial claims and increase in complaints.	M	H	H
6	As a result of the wide-ranging capability of RFR to process large amounts of personal data there is a risk that the processing of personal data may be excessive resulting in regulatory action.	M	H	H
7	As a result of potential incomplete deletion exercises there is a risk that the Reference Image Database may be compiled using custody images which should have been deleted from police systems in line with established retention and deletion procedures this may lead to unwarranted and unjustified damage and distress to individuals.	M	H	H
8	As a result of different scenarios in which a person may be linked to a crime as a suspect there is a risk that the use of RFR to identify that person may not meet the strict necessity threshold and may be unlawful resulting in potential legal challenge, complaints and	M	H	H

	financial penalties or regulatory enforcement action.			
9	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 DPA 2018 resulting in potential regulatory enforcement action and/or financial penalties.	L	H	M
10	There is a risk that officers involved in the use of RFR will have insufficient knowledge of data protection resulting in insufficient consideration of the requirements around the use of RFR and potential breaches of the DPA 2018 which may result in enforcement action, legal action and financial penalties.	M	H	M
11	As a result of lack of training and awareness there is a risk that the Reference Image Database or other data generated by the FRT System is unlawfully disclosed to third parties	L	M	M
12	As a result of technical failure there is a risk that the equipment will not function correctly resulting in incorrect Possible Matches or failure to identify Possible Matches resulting in potential damage and distress or threat risk and harm to others.	L	H	M

Step 6: Identify measures to reduce risk

No.	Measure to reduce or eliminate risk	Risk Treatment	Residual Risk	Measure approved
		Reduce Eliminated Accepted Transferred	L,M,H	Y/N
1	Individuals can apply to SWP/GWP to have their custody image deleted. If the application is granted the corresponding image in the FRT System will also be deleted. The hashing of both data sets will assist this process.	Reduced	L	
2	The RFR Operator will complete Adjudication prior to returning a Match to the Investigating officer.	Reduced	L	

3	A communications strategy will be in place prior to utilising RFR to ensure that all available means of communicating the fact that RFR is taking place via various channels including digital and physical, and information is available to the public on why RFR is effective to ensure that individuals and the public are confident that the decisions made to utilise RFR are based on firm evidence and transparent analysis.	Reduced	L	
4	Where a Match is made, the onus remains with the Investigating Officer to make reasonable enquiries to confirm the identification and should follow up any other information or enquiries that come to their attention, even if those enquiries lead them away from the Match.	Reduced	L	
5	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. Equality Impact Assessments will be completed and regularly reviewed against legal developments. The RFR algorithm utilised by SWP and GWP has been tested by National Physical Laboratory and the findings documented in the NPL Equitability Study. It has been determined that the system is equitable across all demographics and despite testing, no evidence of bias affecting any demographic group tested has been identified.	Reduced	L	
6	The assessments prior to RFR will consider why less intrusive methods are not appropriate and justifying the use of RFR based on investigatory needs.	Reduced	L	
7	The Reference Image Database will include accurate, verifiable images lawfully held or obtained by the police for a law	Reduced	L	

	enforcement purpose at the time of use. No further action will be taken without checks being made on Possible Matches without manual intervention to reduce any damage and distress.			
8	SWP/GWP comply with the National Crime Recording Standards when linking an individual to a crime as a suspect.	Reduced	L	
9	The force will have in place appropriate policy documents for LFR processing under Part 2 and Part 3 of the DPA 2018	Eliminated	L	
10	As part of the RFR training appropriate data protection training will be provided.	Reduced	L	
11	Officers/Staff with access to the Reference Image Database are briefed in respect of circulation of personal information and have been informed that this sensitive data must not be disclosed outside the organisation. Physical and technical security measures are in place (as described in this DPIA) to protect the FRT System.	Reduced	L	
12	The technology has been trialled and tested by SWP. NEC algorithms have also been evaluated by NIST and the Department of Homeland Security and SWP/GWP pays regard to these findings. An RFR Operator, who has been trained in the use of the equipment, including amending the settings to enhance operating parameters. All relevant information is logged for audit purposes. SWP/GWP RFR Documents also outline points relating to the FRT System to ensure that it is used in a way that maximises its effectiveness. The RFR Operator is responsible for continually monitoring and reviewing the system's performance.	Reduced	L	

Step 7: Sign off and record outcomes

Action	Name, position, date	Notes
Measures approved by:	Chief Inspector Scott Lloyd 23.11.2022	Actions must be integrated back into the project plan with completion dates and action owners
Residual Risks approved by	Chief Inspector Scott Lloyd 23.11.2022	If accepting residual high risks, refer to DPO to consider ICO consultation before proceeding
DPO advice provided	Louise Voisey, DPO, 05/06/2023	DPO to advise on compliance, mitigating measures and whether processing can proceed
Summary of DPO advice: I am satisfied that all data protection considerations have been given to the application of RFR by SWP/GWP, with the benefit of insight from the regulators and the courts as to their expectations in terms of lawfulness and privacy. If there is a significant change to the way in which SWP/GWP utilise RFR this DPIA should be revisited to take into consideration any new privacy risk.		
DPO advice accepted or overruled by:	Advice accepted by Chief Superintendent Simon Belcher 29.06.2023	If overruled, an explanation must be provided.
Comments:		
Consultation responses reviewed by:	Chief Inspector Scott Lloyd	If the decision does not align with the views of the consultees please explain

Comments: Document produced in response to information provided by stakeholders		
This DPIA will be kept under review (no later than on an annual basis) by:	Inspector Benjamin Gwyer SWP FRT lead	The DPO should also review ongoing compliance with DPIA.

Annex A – Information Available to the Public

SWP/GWP has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of SWP/GWP to be open and transparent (wherever appropriate and possible) about how data is processed. To this end and having considered the risks to this right posed by the use of RFR, SWP/GWP has adopted a number of measures to ensure that the right to be informed is upheld.

A key measure is the publication of SWP/GWP's Privacy Notices, SWP/GWP policy on protecting special category and criminal convictions, and key SWP/GWP RFR Documents on the SWP/GWP website. Whilst SWP/GWP are not required to publish a number of these documents, it has elected to do so. This is an important measure to inform our communities including those subject to RFR and those who may be placed on a Reference Image Database to understand the standards SWP/GWP, as public bodies, operates to. In doing so, SWP/GWP provides details about when RFR may be used and the considerations and constraints relevant as to who may be placed on a Reference Image Database. In this way, SWP/GWP's use of RFR is both foreseeable and assessable. The published documents provide information as set out in the table below.

Key documents available to the public	Information included
SWP / GWP Privacy Notice:	• Data Controller identity and contact details • Data Protection Officer details • The scope and purposes for processing personal data by SWP/GWP • Data retention periods • Data sharing arrangements • Data security • Rights as a data subject (including access, rectification and erasure) • Complaints (including the right to make a complaint to the ICO and contact details).
SWP/GWP policy on protecting special category and criminal convictions	• SWP/GWP approach in relation to protecting and processing special category and criminal convictions data in relation to the data protection principles • The responsibilities of the Data Controller • Information relating to erasure and retention • How further information may be sought.
SWP/GWP LFR Legal Mandate	• The lawful basis for processing data in relation to RFR. Including in relation to: o Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Protection of Freedoms Act 2012 o Data Protection Act 2018 o UK General Data Protection Regulation o Freedom of Information Act 2000
SWP/GWP Policy Document	• An outline, strategic intent and objectives for the use of RFR and how personal data will be used by the FRT System

	• Key terms used across SWP/GWP RFR Documents • Data retention periods applicable to RFR
SWP/GWP RFR Standard Operating Procedure Processes	• Outlines measures relevant to considering when RFR can be used by SWP/GWP. • Reference Image Database considerations including the basis on which images may be added to a Reference Image Database. • Considerations for Probe Images. • Details concerning the Probe Image submission process including urgent submissions.
SWP/GWP RFR DPIA	• Describes the nature, scope, context and purposes of the processing. • Assesses necessity, proportionality and compliance measures. • Identifies and assesses risk to individuals. • Identifies any additional measures to mitigate those risks.
SWP/GWP RFR Appropriate Policy Documents	• Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the DPA 2018. • Explains how the processing of special category data under Part 2 DPA 2018 and Article 9 General Data Protection Regulation • Explains how SWP/GWP complies with the Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of personal data.

Annex B – RFR Terminology

Within SWP/GWP and throughout the SWP/GWP RFR Documents, the following terms and definitions apply in relation to Retrospective Facial Recognition:-

Adjudication	A human assessment of a potential match generated by the RFR application by an RFR Operator. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors.
Biometric Template	A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm and new templates will need to be generated from the original images if the FRT algorithm is changed.
Candidate Image	Image of a person in the Reference Image Database.
Environmental Factor	They are external element that affect RFR performance such as dim lighting, glare, rain, mist etc.
Facial Recognition Technology (FRT) System Engineer	A person who is deemed to have suitable technical qualifications and experience to optimise and maintain the operational capability of the FRT System.
Facial Recognition (FR) –	The technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database generating probable matches. This is based on digital images (still or from live camera feeds).
Match	A match occurs when the Operator, on viewing the Possible Matches, forms the belief that the Subject is identifiable as the same person shown in the Candidate Image.

No Match	The Operator determines as a result of viewing the Candidate Images and/or Possible Matches that the individual has not been successfully identified.
Probe Image	The facial image or footage submitted for a facial search against the SWP/GWP Reference Image Database.
Possible Match	Operator considers a Candidate Image may be the same person as in the Probe Image resulting in police indices being further searched.
Reference Image Database	A set of lawfully held known Candidate Images which a Probe is searched. For example, a police force's custody image database.
Retrospective Facial Recognition (RFR)	Is a post event use of FRT, which compares still images of faces of unknown Subjects against a Reference Image Database in order to identify them.
RFR Operator	An officer or staff member, who is responsible for establishing the legal basis for using RFR and considering Candidate Images for Possible Matches.
Similarity Score	This is a numerical value indicating the extent of similarity between the Probe and Candidate Image, with a higher score indicating greater points of similarity.
Subject	The individual whose Probe Image is considered for comparison via RFR.
Subject Factor	A factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.
SWP/GWP RFR Documents	SWP/GWP RFR Documents that regulate SWP / GWP use of RFR
System Factor	A factor relating to the FRT System such as the algorithm.

Urgency	In the context of utilising RFR, an Out Of Hours request that is related to an: • Imminent threat-to-life or serious harm situation; and/or • Intelligence / investigative opportunities with limited time to act, where the seriousness and potential benefits support the urgency of action.
Out Of Hours	Any time outside normal business hours 0700 - 2200