# Joint Data Protection Impact Assessment (DPIA) and Information Security Impact Assessment

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 | SWP/GWP | |
| Subject/Title of DPIA | Retrospective Facial Recognition | |
| Name of DPIA adviser | Louise Voisey | |
| Force Information Security Advisor | Lee Bowen | |
| Key dates | Started | |
| | Completed | 28/04/2025 |
| | Review | 19/08/2025 |

| | |
|---|---|
| Project Name | RFR |
| Responsible Owner | ACC Belcher |
| Business Area/Department | Digital Services Division |
| Proposed implementation date | 14/06/2026 |
| Reference No. *(to be allocated by IG)* | AR0120 |

It is recommended that you refer to the DPIA guidance and process documents (hyperlink) to assist in the completion of these sections. Where External Cloud based suppliers are being used please complete Annex A.

Risk matrices are at Annex B

# Step 1: Project Aims and Processing

**Identify why the processing requires a DPIA *(indicate which applies with an 'x')***

| x | Type of processing | Brief details |
|---|---|---|
| | Systematic and extensive profiling | |
| | Public Monitoring | |
| | Denial of Service | |
| x | Data Matching | Biometric templates are matched |
| | Tracking | |
| | Risk of Harm | |
| | Automated Decision Making | |
| | Large scale use of sensitive data | |
| x | Innovative technology | Biometric matching for the purpose of uniquely identifying an individual |
| x | Biometrics | Facial recognition |
| x | Invisible processing | Facial recognition; biometric matching |
| | Targeting children/vulnerable adults | |
| x | Special category/criminal offence data | Biometric data; custody images |
| | Other | |

| Suppliers or sub-contractors | | |
|---|---|---|
| Company details | Name | NEC |
| | Trading name if different | NeoFace |
| | Address | |
| | Main establishment if not in the UK | |
| | Companies House Number | |
| Point of contact | Name | |
| | Role | |
| | E-mail | |
| | Tel. No. | |
| Data Centres | Location (s) | |
| | On prem | |
| | Cloud | |
| Back ups | Location (s) | |
| | On prem | |
| | Cloud | |
| Location of Support and Maintenance | | |
| Procurement stage | | |

**Aims and Objectives**
**Describe the context, purpose and aims of what the processing is intended to do.**

**Aim**

There are increasing demands on policing – financially, resource and high workloads. Great emphasis has been placed on a data driven and preventative approach whilst harnessing new technology and forensics to rebuild public trust. The government has indicated that outdated processes and systems have left the police struggling to keep up with a fast-changing criminal landscape.[1] The Science and Technology in Policing strategy and the National Policing Digital Strategy states that "Central to our objective are plans to modernise core digital systems, putting the power of data and information in the hands of our staff".[2] The National Policing Digital Strategy[3] is clear that increasing officers' operational efficiency is a priority and that a dynamic workforce will be digitally enabled by default, by unlocking value from data, whilst maintaining public trust. This includes ensuring security, ethical and responsible use of data and utilising analytics to extract insights to deliver better outcomes. Technology such as Facial Recognition Technology (FRT) can help the police quickly and accurately identify those wanted for serious crimes, as well as missing or vulnerable people. It also frees up police time and resources, meaning more officers can be out on the beat, engaging with communities and carrying out complex investigations.

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 use of RFR involves the processing of personal data and therefore data protection law applies. The processing of personal data by 'competent authorities' (s.30 Data Protection Act 2018 (DPA)[4]) for 'law enforcement purposes' (s.31 DPA 2018[5]) is covered by Part 3 of the DPA 2018. To note that not all policing purposes fall within the definition of law enforcement purposes e.g. missing persons where there is no suspicion of criminal activity. In such cases, Part 2 DPA will apply.

[1] Home Office on Police Reforms November 2024
[2] S&T in the NPCC's strategy
[3] National-Policing-Digital-Strategy-2020-2030.pdf
[4] Data Protection Act 2018
[5] Data Protection Act 2018

Specifically, the use of RFR for law enforcement purposes constitutes 'sensitive processing' (s.35(8)(b) DPA 2018[6]) as it involves the processing of biometric data for the purpose of uniquely identifying an individual. Such sensitive processing relates to facial images captured and analysed by the software; and must pay particular attention to the requirements of s.35, s.42[7] and s.64 DPA 2018[8].

Sensitive processing occurs irrespective of whether that image yields a match to a person on an Image Reference Database, or the biometric data of unmatched persons is subsequently deleted within a short space of time.

Data protection law applies to the whole process of RFR, from consideration about the necessity and proportionality of using it, the compilation of Image Reference Database, the processing of the biometric data through to the retention and deletion of that data.

**Part 1: Use of RFR**

**Context**

Policing now deals with an ever more transient population, with criminals crossing force borders in order to commit offences and drawing on vulnerable people as victims of crime and also criminal exploitation. A large proportion of offences and matters reported to police, such as suspicious activities that may be preparatory to criminal offences or incidents raising specific concerns relating to the welfare of an individual, are captured on CCTV, whether that CCTV is owned by Police/ Local Authority or captured on cameras/ devices owned by businesses or members of public. Given this ability to move freely, the efficacy of the 'local Officer' to be able to recognise an individual from CCTV recordings or stills becomes increasingly challenging as offenders. Were Officers to undertake searches of images held on Police record management systems based on descriptive identifiers (male or female, weight, height, hair style and colour etc), these searches would likely produce large numbers of responses (given the subjective nature of descriptive indicators) and would require excessive manual processing to determine if an individual is matched. This is also on the basis that an individual has not made attempts to change their appearance since the last time their image was taken. To undertake this process manually would be costly in terms of time and resources, and also excessive in the amount of data being searched, potentially with no outcome at its conclusion.

RFR utilises Facial Recognition Technology (FRT), ingesting a Probe Image or video clip containing the unknown Subject for the purposes of comparison. 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 (SWP) and Gwent Police (GWP), at present this is roughly 676,000 images.
Up to 50 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.

[6] Data Protection Act 2018
[7] Data Protection Act 2018
[8] Data Protection Act 2018

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.

**Necessity**

s.35(5) DPA 2018 requires that where sensitive processing is taking place for a law enforcement purpose without consent it must be:

- Strictly necessary for a law enforcement purpose;
- Meet one of the conditions set out in Schedule 8 DPA 2018[9]; and
- An appropriate policy document must be in place

The public expects the highest standards of compliance by the police and other law enforcement authorities when processing sensitive data. In the ICO's Opinion on Use of Live Facial Recognition in public spaces 'strictly necessary' is described as "'a high bar, but it must be reached before the sensitive processing can take place under Part 3 DPA 2018, i.e. the processing must be more than merely 'necessary' for the law enforcement purpose and cannot be reasonably achieved by a less intrusive method. This recognises that:

- sensitive processing, in this case of biometric data for the purpose of uniquely identifying an individual, is taking place;
- this gives rise to higher risks to individuals' rights; and
- the processing therefore requires higher levels of protections and safeguards.

**Purpose**

The purpose of the processing is provide a post event identification of subjects for a policing purpose. This should only be undertaken in order to progress an investigation where other reasonable enquiries have already been completed, are not reasonably expected to progress the investigation to a point where the individual can be identified, or are not available. RFR will be used to:

a) Support the identification and arrest of people wanted for criminal offences;
b) Support 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);
c) Support the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed.
d) Support the identification of deceased persons, to assist with enquiries on behalf of the coroner.

[9] Data Protection Act 2018

The processing of data via RFR has demonstrated improved efficiencies in the investigative processes and has demonstrable evidence in bringing supporting the identification of persons sought by police in the course of investigations where the occurrence would otherwise be closed and no further investigation would occur as no identification would be made.
RFR offers significant benefit to the police and also to the public in ensuring persons responsible for offences are identified and investigated in an expeditious manner, vulnerable persons are identified and safeguarded and preventative options are considered to reduce vulnerability and risk and reduce further offending and re-offending.

## Requirements for use of RFR

a) For RFR to be used in a lawful and justifiable way, it must be for a clearly defined policing purpose, it must be necessary for RFR to be used in order to progress the investigation (rather than convenient) and must meet a pressing social need. In policing contexts, examples of pressing social need may be:Supporting identification and arrest of people suspected of involvement in criminal offences.

b) 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, etc.)

c) Supporting the identification of persons who may be at risk of serious or immediate harm from others (e.g. Victims of crime, cuckooing, trafficking etc).

d) Supporting the identification of deceased persons, to assist the coroner

**Lawfulness of using Facial Recognition for a policing purpose**

The lawfulness of using facial recognition (albeit Live Facial Recognition) in policing was considered in the case of *R (Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058*[10] in which the Information Commissioner's Office and the Surveillance Camera Commissioner were Interested parties. This also dealt with considerations in relation to interference with Art 8 ECHR, and the Public Sector Equality Duty in relation to the NeoFace Algorithm. The principles set out in that judgment are applied where relevant to use of RFR.

[10] Microsoft Word - R (Bridges) -v- CC South Wales _ors Judgment.docx

The powers of the Police are established in common law. The exercise of these powers should be necessary, proportionate and compatible with human rights[11] and equalities[12] legislation. The misuse of police powers is not normally a criminal offence but is a failure to uphold the policing standards of professional behaviour[13].

Article 8 ECHR

SWP/ GWP acknowledge that obtaining CCTV footage of an individual and processing the image to identify the subject in the image may constitute an interference with the Article 8 right to privacy of an individual or group of people. This DPIA does not cover the capture of images or video via CCTV however it is pertinent in respect of how police then use that image or video, and the subsequent retention of any data or biometric data that occurs as a result of the processing. The process for an investigator to request an RFR comparison has been designed to ensure that sufficient safeguards are included in the process to ensure that any processing that takes place is justified and necessary for the purposes of the investigation, and the processing is clearly linked to the purposes of the investigation in accordance with law.

In *R (on the application of Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058), the Court of Appeal concluded that the Data Protection Act 2018 provided "an important part of the framework in determining whether the interference with the Appellants Article 8 right was in accordance with the law". The application of the Data Protection Act 2018 to RFR is set out in detail in Step 4 below. In addition, the 4-part test in *Bank Mellat v HM Treasury (No2)[2014] AC700*[14] determines whether an interference with Article 8 is proportionate:

1. Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
2. Whether it is rationally connected to the objective;
3. Whether a less intrusive measure could have been used without unacceptably compromising the objective; and
4. Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

This document acknowledges that subject's Article 8 rights are engaged and that RFR may process personal data of individuals not on the Image Reference Database.

In response to the 4-part test referred to above:

[11] https://www.legislation.gov.uk/ukpga/1998/42/section/6
[12] https://www.legislation.gov.uk/ukpga/2010/15/section/149
[13] https://www.legislation.gov.uk/uksi/2020/4/schedule/2/made
[14] https://www.judiciary.uk/wp-content/uploads/2019/03/bank-mellat-v-hmt-final150319docx.pdf

| | |
|---|---|
| Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right | The objective is to identify an individual:<br><br>a) Who is suspected to be involved in the commission of criminal offences.<br><br>b) 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, etc.)<br><br>c) who may be at risk of serious or immediate harm from others (e.g. Victims of crime, cuckooing, trafficking etc).<br><br>d) Supporting the identification of deceased persons, to assist the coroner<br><br>Based on these grounds it is sufficiently important to justify limitation of a fundamental right. |
| Whether it is rationally connected to the objective | A core role of policing is the identification of persons suspected of offences to enable investigations to progress which in turn facilitates the efficient process of criminal justice. There is also an expectation for police to identify persons who are vulnerable and in need of safeguarding or who pose serious risk to themselves or others.<br>RFR processing allows police to identify individuals and respond promptly and proportionately whilst utilising information held on police systems to support informed decision making and risk assessments.<br>The outcomes are the apprehension of persons suspected of offences and protection the wider public safety or, in cases of vulnerable persons in need to safeguarding, to take appropriate actions to safeguard individuals at risk.<br>Were RFR not available, the identifications of these individuals would either be significantly slower, exposing victims and the public to entailial risk of further offences being committed or failure to respond to the needs of an individual which could lead to serious harm, injury, or in the |

| | |
|---|---|
| | most serious cases, death. There is also potential that without RFR, individuals would never be offended and therefore investigations could not be progressed and offenders would continue to commit offences unhindered, leading to loss of confidence in policing, loss or damage to property and injury and risk to members of public.<br>Therefore, the outcome must be that it is rationally connected to the objective |
| Whether a less intrusive measure could have been used without unacceptably compromising the objective | Less intrusive measures are employed as a matter of course i.e. where other feasible lines of enquiry are available to progress an investigation, for example vehicle registrations or details of the potential suspect that would assist with streamlining system searches to realistic levels, these actions are prioritised before RFR processing is requested.<br>RFR is intended to be utilised where reasonable less intrusive enquiries have been exhausted or are not available or likely to advance the investigation, and it is necessary to identify the individual for a policing purpose.<br>Where a policing purpose exists, RFR enables an officer to identify an unknown individual in order to progress lawful policing enquiries and to undertake core policing responsibilities.<br><br>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 |
| Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community. | Based on the information above and technical/organisational controls and measures detailed further in this document, there is a fair balance between the rights of the individual and the wider interests of the community.<br>The processing will facilitate police actions which, if done via traditional measures would require greater intrusion for the individual through potential release of images in attempts to identify the subject via social media or other press releases, or through excessive processing of |

| | |
|---|---|
| | records that are not linked to the subject in an attempt to identify the subject through searching via visible descriptors such as hair colour, perceived height and build etc.<br>It may also lead to individuals who require safeguarding, through the failure to identify persons who have offended against them being able to continue unabated, or through concerns in relation to their welfare not being promptly addressed to ensure their continued safety and welfare. This would likely have more significant impacts in terms of failure to meet core responsibilities expected of policing, and also loss of confidence in policing, increased fear of crime and fear for safety in places that persons would otherwise attend. |

Taking into consideration to answers to the test above, whilst SWP/ GWP acknowledges that Article 8 is engaged, interference is justified in accordance with the law (i.e. police powers under common law.

RFR is a post event use of facial recognition technology, and therefore the necessity for use will be identified as necessary in response to specific information, intelligence, evidence or event. Whilst Police Officers and Staff involved in investigations may request RFR for an occurrence, the RFR Operators undertake specific checks to ensure that other less intrusive lines of enquiry have already been completed or are unavailable to support identification, and also that the purpose of the investigation meets a policing purpose to justify RFR use.

The RFR Operators are specifically trained to consider reasonable expectations of privacy of individuals who may be captured on CCTV but not subject of RFR and take reasonable steps to avoid collateral intrusion, such as using the 'cropping tool' built into the RFR platform.
Any CCTV or image obtained must have been lawfully obtained and held by policing for the purposes of investigations and all reasonable efforts should be made to ensure sensitive processing is no more than is necessary for the purposes of identifying the individual, or individuals, involved for the identified policing purpose. Examples of this would be:

- Identifying the best cameras for the purposes of identification before processing is undertaken
- Cropping the images or video to only include the subject for whom identification is sought

<u>Article 11 (Right to protest)</u>
It should be noted that RFR is not designed or intended to be deployed on large groups of individuals and the policing purposes for RFR do not preclude it being used to identify key individuals in a large crowd, where a policing purpose exists and it is necessary to do so. The risk of unnecessary collateral

intrusion is likely to be greater in large crowds and consideration should be given as to the necessity to identify the subject being balanced against the potential of collateral intrusion being unmanageable in the circumstances.

Where RFR is used at densely crowded locations or locations used for protest/ assembly, it may have an impact upon individuals who are lawfully exercising their human rights under articles: 8 - right to private life, 9 - freedom of thought, belief and religion, 10 - freedom of expression, and 11 - freedom of assembly. Whilst these rights are qualified, this still imposes a duty upon public bodies to ensure that the use of such technologies does not unnecessarily or disproportionately impact the ability of individuals to exercise these rights. It must be recognised in the Judge's ruling in R v Bridges at Divisional Court whereby the level of intrusion of taking a photograph of an individual caused 'negligible' intrusion and the "any impact that has very little weight cannot become weightier simply because other people were also affected".

An example of an occasion where RFR might be used in the context of protest, demonstrations or assembly may be for the purposes of identifying persons who have attended the location for the purposes of causing disorder amongst persons assembling at the location, or where a person who is sought for an offence may enter a location such as a location of religious worship or significance. It would be deemed necessary to identify the subject however it is realistic to consider that persons attending the location may be captured in any CCTV or still images.

Where the decision to utilise RFR in such circumstances is made, RFR Operators should consider all possible options to minimise collateral intrusion. Consideration should be given as to whether other CCTV feeds or camera angles may produce similar results in terms of quality of identification whilst reducing the potential for collateral intrusion. The RFR Operator should then take all reasonable steps to use the cropping tool included to further minimise collateral intrusion.

**Fairness and Transparency**
RFR Operators are reminded of the importance of exhausting all other enquiries available that would be reasonably expected to support an identification before undertaking biometric processing. Investigating Officers are reminded that any action taken must be considered in line with the National Decision-Making Model[15] and the Code of Ethics[16].

**Retention**
The Probe image is retained in line with MOPI for audit purposes in line with the requirements for the investigation. The biometric template associated with the Probe Image is automatically and immediately deleted at the conclusion of the RFR comparison. Where a possible Match occurs, a possible Match report is generated by the RFR Operator and attached to the Occurrence with an Occurrence Log Entry and tasked to the Investigator or associated Investigating Team for further enquiries.

[15] https://www.college.police.uk/app/national-decision-model/national-decision-model
[16] Code of Ethics | College of Policing

**Security**

## Accountability

Governance and oversight of the use of the technology is approached in three stages, as follows:
a) Pre-Operational use;
b) Operational Use
c) Post-use.

### a) Pre – Operational Use

The initial request to make an RFR submission can be made by any member of SWP/GWP staff where there is a policing purpose to justify the need to identify persons within an image or video. The decision to utilise RFR will remain the decision of the RFR Operator.

All submission requests will be recorded by the RFR Operator as will the outcome of those requests.

| SWP/GWP RFR Specific Records | |
|---|---|
| RFR Request | The initial request received by the RFR Operator. Outlines the policing requirement for RFR and the required identifications. |
| RFR Outcomes | For requests submitted via Niche the occurrence OEL will be updated with the outcome of any search.<br><br>For requests received outside of Niche this information will be recorded locally in a secure database. |

A number of other specific SWP / GWP documents pertaining to each SWP / GWP use have been completed centrally. These are set out below: -

| Key documents available to the public | Information included |
|---|---|
| **SWP/GWP RFR Legal Mandate** | • The lawful basis for processing data in relation to RFR. Including in relation to:<br>  ○ Common law policing powers<br>  ○ Human Rights Act 1998<br>  ○ Equality Act 2010<br>  ○ Protection of Freedoms Act 2012<br>  ○ Data Protection Act 2018<br>• Freedom of Information Act 2000 |
| **SWP/GWP RFR Policy Document** | • An outline, strategic intent and objectives for the use of RFR and how personal data will be used by the FRT System<br>• Data retention periods applicable to RFR |
| **SWP/GWP RFR, SOP Processes** | • Outlines measures relevant to considering when RFR can be used by SWP/GWP.<br>  ○ Reference Image Database considerations including the basis on which images may be added to an Image Reference Database. |
| **SWP/GWP RFR Data Protection Impact Assessment (DPIA)** | • Describes the nature, scope, context and purposes of the processing.<br>• Assesses necessity, proportionality and compliance measures.<br>• 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 Data Protection Act (DPA) 2018.<br>• Explains how the processing of special category data under Part 2 DPA 2018 and Article 9 General Data Protection Regulation<br>• 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. |
| **SWP/GWP RFR Equality Impact Assessment** | • Promotes all aspects of equality.<br>• Ensures compliance with the law, taking into account of equality and human rights. |

## b) Operational Use

The FRT System will record the date, time and the submitted Probe Image.

The RFR Operator will ensure that where possible the Probe Image will avoid collateral intrusion and only the Subject of the enquiry will be submitted for RFR.

## c) Post-Use

After each use of RFR, the RFR Operator will record the outcome of the search and advise the Investigating Officer that submitted the image of the outcome.

The outcome of RFR uses must be subject of ongoing evaluation, which in turn should feed into oversight and scrutiny processes.

**Part 2 – Image Reference Database**

Insights indicate that significant criminal offending in South Wales is local and repeat and so comparing potential Probe Images of Subjects against SWP/GWP custody database is considered a relevant tactic when trying to identify a Subject. The custody database contains images of individuals who have been arrested. No victim or witness images are available.

Investigators will not be in a position to anticipate individuals that they may need to identify during the course of their investigations. Whilst it is possible to consider the demographics of an area and the Subject sought for policing purposes, given the capability of persons to move between towns and cities fluidly, it is not realistic to limit comparisons to a geographical area solely on the basis of that being where the incident or event has occurred.
In addition, currently it is not possible to generate lists based on separate categories of subject (e.g. on bail, prison recall etc) due to the fast-paced nature of change in the status of subjects but also due to current technological capability. If it were possible, an officer would be required to have an indication of information which can only be accessible when the subject has been identified.

**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 Image Reference Database will include a Niche nominal number2

**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
☒ Criminal Convictions or offending data
☐ None

Comments:

**Data Subjects**: What categories of data subject are involved?

☒ Persons suspected of having committed or being about to commit a criminal offence
☒ Persons convicted of a criminal offence
☒ Persons who are or may be victims of a criminal offence
☐ Witnesses or other persons with information about offences
☒ Children or vulnerable individuals
☐ Police officers or staff (current and former)
☐ Other

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?

| **Collection** | **PROBE IMAGE:** | **IMAGE REFERENCE DATABASE:** |
|---|---|---|
| Method – manually input. | The technical operation of RFR comprises the following six stages:<br>(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.<br><br>(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. | Where an individual is taken into custody a photograph is taken of them and placed on police systems. Photographs of missing persons will be provided by friends/family or associates and also placed on Police systems. In some cases, images will be provided by other police forces and organisations due to the transient nature of crime and individuals at risk.<br><br>The images are duplicated to create the Image Reference Database for RFR.<br><br>Where an individual has their photograph taken in custody the image will be 'seen' by the FRT system and ingested into the Image Reference Database. |
| Source – by super users | | |
| Privacy Info | | |
| Other Info | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | (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.<br><br>(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.<br><br>(5) Face comparison. The FRT System compares the extracted facial features with those contained in the facial images held on the Reference Image Database.<br><br>(6) Matching. When facial features from two images are compared, the FRT System generates a Similarity Score.<br><br>The supplier of the biometric algorithm and the public sector equality duty in relation to the algorithm has been discussed in the Live Facial Recognition DPIA (256) therefore this will not be covered in this DPIA. The Live Facial Recognition DPIA can be provided on request or is accessible via the SWP Facial Recognition website.<br><br>The security of police systems and devices is not within the scope of this DPIA. | The images are captured for policing purposes and the further processing for the purpose of identifying specific cohorts also for policing purposes is considered to be not to be incompatible with the original purpose**.**<br><br>Due to the changing status of individuals as they move through the justice system it is not currently possible to categorise the images within the database in order to compare the Probe Image of a Subject against a specific cohort, reducing the number of images used in the processing.<br><br>SWP/GWP acknowledge that some images may be unlawfully held. This is a national issue which is currently being addressed by Programme Tabula. |

| **Information flow** | **Description *(provide details where applicable)*** |
|---|---|
| Method of transfer | The Probe image or video is uploaded to the SWP/ GWP digital evidence management system. The RFR Operator downloads the Probe Image and uploads it to the RFR Server where the comparison is undertaken against the SWP/ GWP Custody Image Reference Database |

| | |
|---|---|
| Where to | Secure Facial Recognition Servers within the SWP secure network (DPIA256) |
| Access/permissions | Operators: Operators will only receive access to RFR when they have successfully undertaken training. Access to the RFR NEOFACE platform is restricted to Officers and Police Staff within specific roles where they are required to undertake identification processes and procedures. Permission to use RFR can be removed instantly and remotely should there be any concerns regarding the manner in which the technology is being used by the RFR Operator.<br><br>Facial Recognition Administrators: This is a role-based access provided to a limited number of specifically vetted Officers and staff. These persons will have authorities to make amendments to the Facial Recognition system where specific authority is given and any amendments will be logged and referred to the Facial Recognition Programme Board at the earliest opportunity for agreement or in the event of urgent action being required, escalated to the Senior Responsible Officer for ratification. |
| Aggregation | n/a |
| Sharing | No information processed as a result of the image capture or biometric matching is shared with third parties |
| Storage | The Image Reference Database resides within the SWP Facial Recognition Technology Servers. |
| Retention | Particular to the FRT System<br>• Image of the Subject ('Probe Image') - MOPI retention of personal information<br>• Biometric Template of Probe Image - immediately deleted in the FRT system.<br>• Image Reference Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS |
| Additional information | To ensure the integrity of the images in the custody and missing persons database and the duplicate Image Reference Database on the Facial recognition Servers, each image is applied a hash value which is compared on a daily basis. |
| Recorded | |
| Additional integrated technologies | FRT Technology (DPIA256), Niche RMS, Image Reference Database |
| Auto delete/Manual deletion/overwrite | See retention above.<br>The hash values on the image reference database will alert the FRT Project Team to any variances in the database e.g. an approved request for deletion of a custody image ensuring that image is removed. |

| | |
|---|---|
| Additional information about the process | All actions can be audited, and the information is monitored and evaluated to identify issues, measure success and ensure regulatory/legislative compliance of RFR.<br>Appropriate Police Documents will be available.<br>Detailed Standard Operating Procedures and training will be provided to RFR Operators. |
| Diagram or process map | |

| **How will the information be used?** | |
|---|---|
| | Monitored in real time to detect and respond to unlawful activities |
| | Monitored in real time to track suspicious persons/activity |
| x | Compared to reference data of persons of interest through processing of biometric data such as facial recognition |
| | Compared to reference data of vehicles of interest through ANPR software |
| | Linked to sensor technology |
| | Used to search for vulnerable persons |
| | Used to search for wanted persons |
| | Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies |
| | Recorded data disclosed to authorised agencies to provide intelligence |
| | Other: *(please specify below)* |
| | |

**Describe the context of the processing:**
*Who will be making decisions about the uses of the system and which other parties are likely to be involved?*
*Will you be sharing the information with other organisations or agencies? Records any other parties you would disclose the data to, for what purposes*
*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?* |
|---|
| The use of the system has been determined by SWP/GWP to supplement existing police powers to identify individuals where a policing purpose exists. The initial request to make an RFR submission can be made by any member of SWP/GWP staff where there is a policing purpose to justify the need to identify persons within an image or video. The decision to utilise RFR will remain the decision of the RFR Operator, who will be trained in the appropriate and proportionate use of RFR, the Code of Ethics and the National Decision-Making Model. As set out above the decisions will be auditable and evaluated.<br><br>No information processed for the purpose of uniquely identifying an individual via RFR will be shared with any third parties. This is a supplemental tool for existing policing purposes.<br><br>The police have common law powers which are deployed for policing purposes which are generally defined as:<br><br>• protecting life and property,<br>• preserving order,<br>• preventing the commission of offences,<br>• bringing offenders to justice, and<br>• any duty or responsibility of the police arising from common or statute law<br><br><u>Children and Vulnerable People</u><br><br>The retention of images of children on the Image Reference Database are subject to shorter retention periods under the Management of Police Information (MoPI)<br><br><u>Welfare and Safeguarding of Children and Vulnerable People</u><br>If the Subject of RFR use is found in circumstances that suggest their welfare and safety may be at risk, force safeguarding procedures should be initiated. This is especially pertinent for Children and vulnerable persons (as defined by College of Policing).<br>It is recognised that children under the age of criminal responsibility may be used by older children and adults to hold illegal items such as drugs and weapons and, in some cases, firearms or to undertake criminal activity for the criminal benefit of others. This criminal exploitation is often:<br>• in the hope that police may not suspect they are in possession of illegal items (knowingly or otherwise);<br>• knowing that if criminal offences are identified involving children or vulnerable people, they cannot be prosecuted for criminal offences. |

Lawfulness - Civil Liberties groups have previously raised concerns about the use of biometric facial matching in law enforcement. These concerns have been addressed in part following the *Bridges* cases however RFR is subject of request by the Investigator and support of the RFR Operator with their specific knowledge. RFR is not subject to the oversight and approvals that precede deployments of Live Facial Recognition.

Interference with Human Rights - It is acknowledged that it is likely that use of RFR may interfere with the fundamental right to privacy. The application of the Bank-Mellat 4-part test (above) supports the findings of the court in *Bridges* that use of facial recognition can be deployed for policing purposes in accordance with the law and therefore such interference can be justified.
Reference to Article 11 is included in the sections above however for ease of reference RFR is not designed to be used in densely populated locations and is intended to process only one face contained in an image. Where collateral images are captured in the background the officer will crop the image to remove any others.

Function Creep – there are concerns RFR will be used to monitor movements and actions of the public with no justification or may be used covertly.

Disproportionality regarding the Image Reference Database – there are concerns that comparing a Subject's biometric template against the entire custody database is disproportionate. This is explained above. Due to the transient nature of criminals and the fast changing status of those within the Justice system it is not currently possible to categorise the images. This may also negate the benefits of effective policing in a more timely manner benefitting the wider public and those at risk.

In order to best serve the public and in particular victims, realising swift and effective justice is a considerable aim. It would be almost impossible for any one police officer to be able to identify effectively an unknown individual from potentially thousands of individuals from their face alone; use of RFR assists the front-line officer identify, help or dismiss a Subject from their enquiries. This also removes the potential for disproportionate processing of information relating to persons who are not related to the Subject for the purposes of ascertaining the identification of the Subject for a policing purpose. To undertake this manually would be both disproportionate in terms of the amount of data an Investigator would need to review the purposes of identification.

**Benefits and Impacts:**
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? Are there any adverse effects from the processing?

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.

RFR is a post event use of FRT, where a policing purpose to identify a subject has already been identified. This allows comparison of a Probe Image of the subject to be compared quickly against the custody database and allows for informed decision making in plans to respond to crime and to keep members of the public safe. This offers significant benefit to the police, other public services, the wider public, victims of crime and those in need of urgent help.
The impact RFR would have on resourcing and demand by enabling more time to be spent in critical areas rather than administrative efforts to consult numerous records and personally identifiable data would be beneficial to all.

There is minimal impact on the Subjects whose data is being processed. There will be more tangible impact on the individual if RFR is not used, in terms of privacy, time, safety, justice or retention and accessing/viewing of personal data in available records whilst trying to identify a Subject.

In relation to deceased Subjects, RFR will assist in identifying the Subject to allow for the expeditious notification of a next of kin and formal identification for Coroner's investigations. This will also reduce the number of occasions on which a potential next of kin is incorrectly sought to identify a Subject.

## Step 3: Consultation

List the relevant stakeholders who have been consulted *(please indicate whether stakeholder is internal or external and their role/interest)*

| Stakeholder consulted | Consultation method | Views raised | Measures taken |
|---|---|---|---|
| Information Commissioner's Office | | Advice and guidance was received from the ICO.<br>Opinion on Deployment of Live Facial recognition in public places and interested party in<br>(on the application of Edward Bridges) v Chief Constable of South Wales Police [2020]<br>EWCA Civ 1058.<br>Whilst the guidance related to LFR, there was wider discussion as to the lawfulness of FRT, which includes RFR, in law enforcement. | |
| Information Commissioner's Office | | . In 2019 the ICO commissioned a report on use of LFR for law enforcement purposes in which the following public opinions were obtained:<br>• 82% of those surveyed indicated that it was acceptable for the police to use LFR;<br>• 72% of those surveyed agreed or strongly agreed that LFR should be used on a permanent basis in areas of high crime;<br>• 65% of those surveyed agreed or strongly agreed that LFR is a necessary | |

| | | | |
|---|---|---|---|
| | | security measure to prevent low-level crime; and<br>• 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.<br><br>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.<br><br>58% of those surveyed thought it was acceptable to be stopped by the police in such circumstances, while 30% thought it was unacceptable.<br><br>Whilst this public perception survey considered LFR, it still provides guidance on public support for FRT in law enforcement, and the processing of large groups in order to locate a subject of interest. | |
| 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. | |
| Home Office Biometrics Programme (HOBs) | | Additional guidance in support of the above from the HOB lead on Privacy | |

| | | | |
|---|---|---|---|
| | | Impact assessments (Now referred to as Data Protection Impact Assessments or DPIAs) | |
| South Wales Police Independent Ethics Committee | | Early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities. | |
| 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. | |
| Leicester Police | | Professional discussions over their previous use of slow-time recognition functionality in the preparatory phase of our project implementation | |
| National Police Chiefs Council | | Professional discussion and advice over the development of the project in its phases and the use of custody image. | |
| 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. | |
| Police Digital Service | | Professional discussions over system developments against a desired national rollout picture of the future. | |

| | | | |
|---|---|---|---|
| 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 | |
| Strategic Facial Matcher (SFM) | | Guidance in support of new platform anticipated 2024 | |
| 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" | |
| 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"<br><br>Whilst this Panel discussion related to LFR, indications of public perception and also on the application of legislation to FRT in law enforcement such as data protection and human rights remains relevant to RFR. | |
| Publication consultation sessions have been completed at various locations across South Wales Police force area since the development of FRT within SWP. | | There have been workshops delivered at SWP HQ and also at other force events.<br><br>There has been ongoing public engagement and consultation during Deployments of LFR wherein all aspects of FRT are discussed and where possible to do so, demonstrated utilising test databases and Probe Images.<br><br>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 | |
| 'Is there a legitimate role for facial recognition in policing and law enforcement' at the London School of | | Participation by Chief Constable Jeremy Vaughan in the SCC/BC event. | |

| | | | |
|---|---|---|---|
| Economics on the 14th June 2022. | | Attendance included academics, technologists, representation from civil libertarian groups and broader society | |
| South Wales Police Ethics Committee | | March 2025 – Overview of South Wales Police use of FRT covering all 3 forms of FRT and how each form of FRT is deployed and utilised in a policing context. | |

## 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<br>Part 2 will be applied to general processing i.e. missing persons where no criminal investigation is being undertaken<br>Part 3 will be applied to Law Enforcement Processing<br><br>To note policing purposes are covered by both Part 2 and Part 3 | |
| Legal power to carry out processing e.g. statute, common law, court order etc. *(please provide details)* | Common law powers<br>Police and Criminal Evidence Act 1984<br><br>Interference with Article 8 is addressed above. | |
| Lawful basis for processing *(please select the appropriate conditions. If different conditions apply to different stages of the processing please provide further details)* | **General: Personal data**<br><br>☐ Consent<br>☐ Contract | **General: Special category data**<br><br>☐ Explicit Consent<br>☐ Obligations & rights in employment, social security & social protection law |

| | | |
|---|---|---|
| ***General Processing (GDPR)**:*<br>*Please select one condition for processing personal data. If processing special category data please select a further condition.*<br><br>*ICO Guide to GDPR - Lawful Conditions for processing* | ☒ Vital Interests<br>☐ Legal Obligation<br>☒ Public Task<br>☐ Legitimate Interests | ☒ Vital interests<br>☐ Members of former members of a not-for-profit body<br>☐ Data has been made manifestly public by the data subject<br>☐ Legal claims<br>☒ Substantial public interest<br>☐ Health<br>☐ Public interest in Public Health<br>☐ Archiving |
| *Law Enforcement Processing:*<br>*Please select one condition for processing personal data only.*<br>*If sensitive processing takes place please select a further condition.*<br><br>*ICO Guide to Law Enforcement Conditions* | **Law Enforcement: Personal data**<br><br>☐ Consent<br>☒ Processing is necessary for the performance of a task carried out for that purpose by a competent authority. | **Law Enforcement: Sensitive processing**<br><br>☐ Consent<br>☒ Processing is strictly necessary for the law enforcement purpose; **and**<br><br>☒ Statutory etc purposes<br>☒ Administration of justice<br>☒ Protecting vital interests<br>☒ Safeguarding of children and individuals at risk<br>☐ Personal data already in the public domain<br>☐ Legal claims<br>☐ Judicial Acts<br>☐ Archiving |

| | | |
|---|---|---|
| | | |
| Data Protection Act 2018 Schedule conditions for processing special processing or in the substantial public interest | Schedule 1 Special Categories of Personal Data and Criminal Convictions<br><br>Part 2 Substantial Public Interest Conditions<br>Para 5 Requirement for an appropriate Policy Document<br>Para 6 Statutory etc, and government purposes<br>Para 7 Administration of Justice<br>Para 10 Preventing or detecting unlawful acts<br>Para 18 Safeguarding of children and of individuals at risk<br><br>Part 3 Additional Conditions Relating to Criminal Convictions<br>Para 30 Protecting individual's vital interests<br>Para 36 Extension of conditions in Part 2 of this Schedule referring to substantial interest<br><br>Part 4 Appropriate Policy Documents and additional safeguards<br><br>Schedule 8 (1) Statutory etc purposes<br>Schedule 8 (3) Protecting individuals' vital interests<br>Schedule 8 (4) Safeguarding of children and individuals at risk | |

<table>
<tr><td>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.<br><br>If no privacy information is to be provided, please provide the reason for this.</td><td>This DPIA considers the utilisation of RFR and will be supported by a Communications Strategy to provide information to the Public.<br><br>Privacy notices are available on the SWP/GWP website alongside a direct link to this via the South Wales Police/ Gwent Police Facial Recognition websites.</td></tr>
<tr><td>Will the personal data collected be used for any other purposes? (Please provide details)</td><td>No. The image is retained as part of an audit process and for the purposes of the investigation for which it was originally obtained however the biometric template of the Probe Image is immediately deleted at the conclusion of the RFR comparison.</td></tr>
<tr><td>Will the processing include mechanism to facilitate the exercise of individual rights (please select which rights can be exercised)</td><td>
<table>
<tr><td>Right to be informed</td><td>x</td><td>Right to restriction of processing</td><td>x</td></tr>
<tr><td>Right of access by data subject</td><td>x</td><td>Notification of erasure, restriction or rectification</td><td>x</td></tr>
<tr><td>Right to rectification</td><td>x</td><td>Right to data portability</td><td></td></tr>
<tr><td rowspan="2">Right to erasure (right to be forgotten)</td><td rowspan="2">x</td><td>Right to object</td><td>x</td></tr>
<tr><td>Automated decision making, including profiling</td><td></td></tr>
</table>
</td></tr>
<tr><td>How will you ensure that the data being processed is accurate and up-to-date? Will the processing allow you to erase or rectify inaccurate data without delay?</td><td>Subjects – processing will be post event.<br>Initial user validation in a non-live environment has been conducted.<br>In excess of 400 controlled searches were carried out. On all occasions when the Probe Image is of a Subject that exists in the Image Reference Databases the correct Candidate Image is returned to the RFR Operator in position number 1.<br>The validation process focuses on any potential age, gender and ethnic imbalance. These concerns have been mitigated during the validation period and independent academic equitability testing undertaken by the National Physical Laboratory (NPL) has shown that there is no identifiable bias across any of the demographics tested, with equitability being seen across all groups tested.<br>A link to the findings of the NPL study can be accessed via:<br>frt-equitability-study_mar2023.pdf (science.police.uk)</td></tr>
</table>

| | |
|---|---|
| | There will also be manual consideration of Possible Matches by an RFR Operator and the Investigator prior to any action being taken.<br>As part of the Force procurement process, due diligence must be given to expected algorithm performance (or accuracy). The National Institute of Standards & Technology 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.<br><br>The SWP/GWP supplier has also been held in high regard by the NIST in its 2019 evaluation of over 200 algorithms.<br><br>Data will be checked against source SWP/GWP databases, managed in accordance with MOPI standards. These databases are kept up to date as required for effective law enforcement so that personal data which is known to be inaccurate, materially incomplete or no longer up to date is not transmitted.<br><br>The core source database is Niche RMS which undergoes rigorous checks and balances to ensure the data is accurate and fit for purpose. The software company does not have access to data held in the record management system or the ability to alter, amend or delete data held.<br>Niche RMS makes clear distinctions between different categories of subject (e.g. suspects, persons convicted, victims, witnesses) and is available to the Investigator following the RFR Match being returned for consideration against all other evidence. The expectation is that the Investigator will consider the Match critically against the other evidence available, even if other evidence leads them away from the Match returned.<br><br>SWP/GWP personnel will take all reasonable steps to ensure that each image on an Image Reference Database does actually pertain to the intended person. No action will be taken against a Subject without human consideration of a Possible Match.<br><br>The Image Reference Database has an applied hash value to maintain the integrity of the database from the custody database. Any variations in the hash value is notified to the Project team for rectification. |

| | | |
|---|---|---|
| | Custody Images are subject to a national review – Programme Tabula<br><br>Individuals whose data is held on police systems can make a request for deletion which is under the discretion of Chief Constables. | |
| Does the processing require you to keep the information in an identifiable form? *(If yes, please provide reasons for this)*<br><br>Could you pseudonymise or anonymise the data to achieve your aim? | The initial image and biometric template of the subject is not identifiable. The processing of the biometric template is for the purpose of uniquely identifying a living individual and is therefore considered to be special category data.<br><br>The result of a positive and confirmed match will be retained will need to be identifiable so that the policing purpose/law enforcement purpose can be fulfilled.<br><br>Any retention beyond RFR use will be in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and/or in accordance with SWP/GWP's complaints / conduct investigation policies.<br><br>Technical systems and standard operating procedures help ensure that data is properly retained or deleted.<br>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.<br><br>The Candidate Images on the Image Reference Databases need to be identifiable to the police and cannot be anonymised or pseudonymised to achieve the aim of the RFR use. | |
| Retention | How long will the data be retained in an identifiable form? | The biometric templates of the Probe Image will not be retained.<br>The Probe Image is retained in accordance with Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and/or in accordance with SWP/GWP's complaints / conduct investigation policies. This is for the purposes of investigation only. |

| | | |
|---|---|---|
| | | The Candidate Images on the Image Reference database are retained in accordance with Management of Police Information (MoPI) retention periods. |
| | Why is the data retained for this period? | Custody Images are retained in accordance with Management of Police Information retention periods. |
| | What reviews of the data will take place? | Reviews of custody images are undertaken in accordance with Management of Police Information retention periods. |
| | How will the data be disposed of? | The biometric templates of the Probe Images are disposed of automatically and immediately on conclusion of RFR use.<br>Custody images are removed from police systems.<br>The Image Reference Database is a replica of the images on police systems with an applied hash value to enable to the Facial Recognition team to identify images for removal |
| | Are backups subject to the same process as above? | Yes |
| | If not, please provide details | |
| How will you ensure that the processing is limited to its lawful purpose and that only the minimum data that is necessary for that purpose is captured? | This detail is captured in the Policy document however replicated below for ease of review. The below process outlines the necessary steps for RFR use and assessments and tools available to RFR Operators to ensure processing is lawful, necessary and minimised to the purposes for which it is required.<br><br>The standard end-to-end process of an RFR use can be summarised as follows: -<br><br>a) Submission is made via a Niche workflow, secure email, evidence management system or encrypted USB drive to the SWP Identification (ID) unit.<br><br>b) The RFR Operator will ensure the enforcement purpose identified, safeguards considered, and correct Image Reference Database identified. | |

<table>
<tr><td></td><td colspan="2">c) The RFR Operator will review the image(s) or video and select the most appropriate Probe Image or probe video dependant on the Environmental and System Factors. Where possible to do so, the RFR Operator should crop the image using the cropping tool within the RFR system to only include the face of the subject individual. The RFR Operator may also, where necessary, adjust the properties of the image such as lighting and orientation and scale.<br><br>d) The Probe Image or video is then submitted for processing by the FRT System. If the FRT system can correctly locate a face within the submission a comparison is made against the Image Reference Database. Where no face is recognised by the FRT System, an error is displayed the RFR Operator can either amend the image or image thresholds to attempt to locate a face.<br><br>e) The FRT System will then generate a list of the most similar 50 Candidate Images. These Possible Matches are then reviewed by the RFR Operator for likenesses. Where necessary they can utilise the FRT System to compare the images in a variety of different ways. (Side by side, Overlays etc)<br><br>f) The RFR Operator will consider the Possible Match, noting the FRT System, Subject and Environmental Factors, locally held intelligence and together with the benefit of their experience and training, they will determine if a Match has been made.<br><br>g) Any result is then passed to the investigating officer via a Niche workflow.<br><br>h) A record of the search and the outcome is recorded by the RFR Operator.<br><br>i) The Investigating Officer will review the Match to determine that they are satisfied it is accurate and that it matches with any descriptions received during the investigation. The Investigating Officer should undertake further enquiries to ensure there are reasonable grounds to support any further action. Officers should also make any enquiries that might lead them away from the person identified.</td></tr>
<tr><td rowspan="5">Transfers outside the UK</td><td>Location and recipient details</td><td>n/a</td></tr>
<tr><td>Environment (e.g. on premise, cloud)</td><td rowspan="4"></td></tr>
<tr><td>Reason for transfer</td></tr>
<tr><td>Safeguards</td></tr>
<tr><td>Does the above also apply to any backups?</td></tr>
</table>

| | |
|---|---|
| | If not, please provide details [redacted] |
| Information Sharing | No personal information will be shared with third parties.<br><br>Information regarding the monitoring and evaluation of RFR use will be shared with academic partners and evaluators and the National Biometric Strategy Board and NPCC Facial Recognition Technology Board. Membership of these boards includes interested regulators and commissioners, to include the Biometrics Commissioner, Information Commissioner, Surveillance Camera Commissioner, Forensic Science Regulator and the National Police Chief Scientific Adviser.<br><br>A contract is in place with the algorithm supplier. |
| **Information Security** | |
| What police system(s) is involved in this processing? | Niche RMS, Facial Recognition Technology Servers (SWP on premise) |
| Is data encrypted in transit? If yes provide details | Yes, the information is transferred between systems on an accredited secure closed VPN. |
| Is data encrypted at rest? If yes provide details | Yes, any information is stored on systems an accredited secure closed VPN. |
| What access controls are in place? If yes, please provide details of who will have access to data and what controls will be in place? | Access to the RFR system is only provided to Police Officers and Staff in specialist roles requiring identifications to be undertaken. Access to the RFR platform is only provided on the completion of training and refresher inputs are offered to staff periodically. If there are any concerns raised regarding the manner and use of RFR by the RFR Operator, permission to use RFR can be removed with immediate effect and remotely until such a time as those concerns have been addressed.<br><br>Access to NICHE RMS to obtain further information following a positive match is assigned to officers and staff dependant on their role, vetting and training.<br>Access to the FRT System and supporting source databases utilises roles to assign privileges. This means that individuals can be assigned levels of access based on a permission level, the higher the permission level will allow the individual greater access to change application settings. |

| | |
|---|---|
| | Internal governance arrangements have been established for RFR with governance and accountability provided by the Facial Recognition Technology and Biometric Board. Onward accountability is provided by the allocation of a Senior Responsible Officer (SRO).<br><br>The data is held securely on SWP/GWP 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. The data held on SWP/GWP systems is not specific to RFR (it provides RFR with the information needed to compile and generate Image Reference Database(s) and relates to policing information generated following the use of RFR). |
| Is the force data segregated? Provide details | n/a |
| What audit arrangements are in place for use of the system? | The application has an in built and robust audit file log CSV file (hashed).<br>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<br><br>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. |
| What training will be provided to users? | Annual Management of Police Information and Data Protection training is mandatory for all staff and officers<br>SWP/GWP RFR Documents provide for the training of officers and staff involved in RFR . The training helps ensure role specific:<br>1. familiarity with SWP/GWP RFR Documents;<br>2. knowledge of RFR use;<br>3. understanding of the lawful processing of personal data in accordance with the DPA 2018;<br>4. understanding the scope of the Regulation of Investigatory Power Act 2000;<br>5. knowledge of police powers and how they may apply when responding to Matches;<br>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 |
| Level of vetting for contractors (including support & maintenance) | Operating staff will all be vetted and cleared to at least MV/SC level. |

| | | |
|---|---|---|
| Details of security measures in place where data is held | Local arrangements for police systems are in place. | |
| How will the product connect to police systems? | Via Secure API within the SWP Secure network | |
| Data held on third party systems<br><br>*(Redacted results of penetration testing will need to be provided)* | Penetration test conducted? | n/a |
| | Date of last penetration test? | [redacted] |
| | Has system been subject to a security breach? | |
| SOC *(Third party cloud based only)* | Does third party have SOC accreditation? | |
| Certifications *(e.g. ISO27001, provide details including scope – copies to be provided)* | [redacted] | |
| Has the Joint Supplier Questionnaire been completed? | | |

| **What other less intrusive options have been considered?** | |
|---|---|
| **Solution** | **Reason why this is not suitable** |
| n/a | Traditional methods are resource intensive and not efficient |
| | |
| | |
| | |

| **Policies -*are there written policies specifying the following*** | | |
|---|---|---|
| **X** | **Requirement** | **Details** |
| | Agencies/organisations that are granted access | |
| x | How information is disclosed | RFR Policy, SOPS, Overarching Privacy Policy, Privacy Notices |
| x | How information is handled | RFR Policy, SOPS, Overarching Privacy Policy, Privacy Notices |
| Y/N | | |
| Y | Are these made public?? | Privacy notices are public facing |
| Y | Are there auditing mechanisms? | All RFR searches, whether leading to a Match or No Match are concluded with the RFR Operator placing an entry on the occurrence log of the |

| | | |
|---|---|---|
| | | investigation the comparison was sought for. The RFR system also has an audit function whereby actions of the RFR Operator can be reviewed if concerns are raised in regard to their use of the system or the manner in which they are using it. |
| | If so, please specify what is audited and how often | Divisional management oversight will fall in line with similar review periods to monitor compliance and outcomes.<br><br>Force level scrutiny boards will review the data at least quarterly to ensure that scrutiny is sufficient and that sufficient oversight is in place to ensure effective management of the use of this technology.<br><br>FRT Programme Board will assess the effectiveness of use of RFR including consideration of accuracy and potential bias in RFR comparisons in uncontrolled operational environments (varying lighting conditions, image quality and other factors that could affect the reliability of results returned), outcomes of the comparisons and reviews of perceived benefits of use. |

| Step 5: Identify and assess privacy & compliance risks *Please identify all risks for each section* | | | | | | | |
|---|---|---|---|---|---|---|---|
| **No.** | **Identify risk – Cause, event, effect** | **Likelihood (L, M, H)** | **Impact (L, M, H)** | **Risk (L, M, H)** | **Mitigating measure** | **Residual Risk (L, M, H)** | **Accepted/ Rejected** |
| **R1**<br>**Vulnerability when data in transit**<br><br>(Consider risk from various threats from hackers such as Foreign Intelligence services, Serious and Organised Crime, and individual hackers for example, force data transiting networks should be adequately protected against tampering and eavesdropping) | As a result of the biometric template being transferred from the device the RFR Operator is using to the SWP FRT servers there is a risk that it could be intercepted or interfered with by threat actors leading to a compromise of the data and/or threat to police systems which in turn could affect the confidentiality, availability and integrity of all police held information | L | H | M | RFR uses on prem servers are all within the secure SWP VPN. RFR can only be accessed via authorised SWP devices. Force issued mobile devices are encrypted and have multiple password/PIN access requirements and timeout screen locks. Devices can be deactivated and wiped remotely. No data is transferred outside of this network which is accredited to national security standards | L | |
| **R2**<br>**Vulnerability when data at rest**<br><br>(Consider risk from various threats from hackers such as Foreign Intelligence services, Serious and Organised Crime, and individual | As a result of information being stored on mobile devices such as laptops there is a risk that it could be accessed, there is a risk that it could be intercepted or interfered with by threat actors | L | H | M | RFR uses on prem servers are all within the secure SWP VPN. No data is stored outside of this network which is accredited to | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| hackers for example. A malicious or compromised user of the service should not be able to affect the service or data of another. | leading to a compromise of the data and/or threat to police systems which in turn could affect the confidentiality, availability and integrity of all police held information | | | | national security standards. Force issued mobile devices are encrypted and have multiple password/PIN access requirements and timeout screen locks. Devices can be deactivated and wiped remotely. No images or biometric data is stored on the device. All information is within the force secure network. | | |
| **R3**<br>**Physical Security**<br><br>(Force data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure by malicious or disaffected individuals who have indirect access to information; An individual who has no authorised access to police business information/ system, such as a cleaner, maintenance personal) | There is a risk that an individual may seize a force issued laptop from an RFR Operator resulting in unauthorised access to information which may pose a risk to others. | M | M | M | In the event that this occurs when an RFR Operator is utilising RFR there are no personal details available even at the point of a positive match. The biometric data will not be available to the individual and access to further information requires additional authentication before the screen timeouts and locks rendering it inaccessible to unauthorised individuals. | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | There is a risk that members of the public or the subject may suffer physical harm if RFR is not used leading to a delay in critical information being accessed resulting in physical harm | H | H | | RFR is a post event use of FRT. Whilst the amount of time to have passed is not defined, there will be cases where RFR is required urgently for matters of protecting vulnerable persons at risk of harm, identifying offenders who pose significant risk or identifying persons suspected of planning or preparing acts of terrorism, extremism or serious organised crime that could have serious consequences upon the lives and safety of others.<br>For this reason, processes for dealing with urgent requests for RFR are established within SWP/ GWP capabilities where required in order to ensure an effective response where required. | L | |
| **R4**<br>**Personnel Security**<br><br>(Malicious or Disaffected individuals who have direct access to information; An individual who has | There is a risk that force officers or staff may use RFR to identify individuals where it is not necessary for a policing purpose leading to unlawful processing of | L | M | M | Only a small cohort of trained Officers and staff have access to RFR.<br>Whilst it is recognised that any member of | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| authorised access to police business information/system, such as approved user with limited privileges) | personal and special category data resulting in loss of confidentiality. | | | | SWP involved in investigations (Officers or Staff) can request RFR, the RFR Operator still has the autonomy to decline a request if a policing purpose is not made out or if other less intrusive enquiries that would reasonably achieve the outcome of providing an identification are available.<br><br>Use of the RFR system is auditable where required and if concerns become apparent in relation to the use of RFR by an RFR Operator, their access to the system can be removed remotely and immediately until such time as the concerns have been addressed. | | |
| **R5**<br>**Malicious or Disaffected individuals who have privileged access to information;**<br><br>(An individual who has privileged authorised access to police business information/system, such as IT administrator/system owner) | As R4 | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **R6**<br>**Commercial Service Providers/ Suppliers**<br><br>(Access to systems and information through an attack by the employees of the service provider either malicious or accidental. Consider how 3rd party accesses service for maintained for example.). | There is a risk that the supplier of the algorithm may fail to ensure that any bias or discrimination is eliminated as far as possible resulting in inaccurate identification of individuals leading to false arrests, unlawful interference with Article 8 rights, and targeting of minorities unfairly | L | H | M | The algorithm was tested by National Physical laboratory to determine the most appropriate settings to mitigate or eliminate bias towards any demographic. Whilst this testing attempted to replicate the realism of operational environments, it is recognised that there are variables such as lighting etc in the operational environment that cannot be controlled and could not be tested in a non-operational environment.<br>The Facial Recognition Project Team monitor searches to assess system accuracy and identify any potential bias or factors that might impact the accuracy or bias within the system..<br>This will include a review of the number of searches returning positive matches, those returning negative matches, | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | the conditions prevalent the Probe Images (conditions/ locations etc) Matches returned to Investigators by the RFR Operators. | | |
| | There is a risk that the supplier may gain access to the data used for RFR resulting in compromise and loss of confidentiality leading to a loss of public confidence and trust | L | H | M | The supplier does not have access to any SWP/GWP information or any data captured or used as part of RFR | L | |
| **R7**<br>**Accidental Disclosure**<br><br>(The disclosure of information by staff either by careless talk or by allowing police business information to be viewed by unauthorised persons, through inadequately trained or inexperienced staff) | As a result of the Operator identifying an incorrect match there is a risk that third party data may be disclosed leading to a loss of confidentiality | L | M | M | The RFR Operator does not disclose any data. A potential Match is passed to the Investigator who will not solely rely on the images presented to confirm any additional details. RFR is an aid to identification however the officer will consider all evidence available to corroborate the Match . No action will be taken on the basis of an image. | L | |
| **R8**<br>**Environmental threat**<br><br>(Risk of fire, flood, explosion etc.) | | | | | | | |
| **R9**<br>**Other** | As a result of RFR use there is a risk that fair processing information may not be widely available to members of the public | L | H | M | The Privacy notice provides details in relation to biometric processing. This is | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (explain other threats that have been identified as part of the Risk Assessment process) | resulting in them not being informed of the processing of their personal data resulting in a potential data breach, increased complaints, court cases, enforcement action and reputational damage | | | | available on the SWP/ GWP public facing website and there are links to this data via the SWP/ GWP Facial Recognition Technology pages.<br><br>SWP/ GWP periodically post articles and 'good news stories' on social media relating to the use of RFR which often include links to more information about Facial Recognition Technology and privacy notices. | | |
| | As a result of RFR use there is a risk that it may contravene the right to privacy or deter members of the public from exercising their right to freedom of assembly and freedom of expression afforded by the Human Rights Act and that any limitation on these rights is not in accordance with the law resulting in potential legal challenge, financial claims and increase in complaints | M | H | M | RFR is a post event use of FRT. Based on this, it is reasonable to consider that information should be available to the Investigator and the RFR Operator to make a determination as to whether the interference with the rights of individuals | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | who may have attended a location is proportionate and necessary. There should also be consideration as to whether less intrusive means could be considered, for example utilising CCTV from a different location where the chances of collateral intrusion are less, or where other enquiries might be available to support the investigation.<br><br>RFR Operators are trained to utilise the cropping tool to reduce or eliminate collateral intrusion and RFR comparisons should only be undertaken of individuals who are suspected or known to be linked to the policing purpose for which the RFR comparison is requested.<br><br>Use of RFR is scrutinised at numerous levels | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | within SWP/ GWP to ensure that it is fit for purpose and utilised in an ethical and proportionate manner. | | |
| | As a result of incorrect matching there is a risk that an individual may be incorrectly arrested leading to loss of liberty, complaints and enforcement action | L | H | M | A decision to arrest a subject is not solely based on a facial image match.<br><br>If the Probe Image is incorrectly matched against Image Reference Database this may result in an unlawful arrest.<br><br>RFR Operators receive specific training in regard to assessing quality of the Probe Image and also assessing Matches to determine if a Match is made.<br><br>There is a second fail safe in the RFR process being the Investigator. The RFR Operator returns a possible Match to the Investigator to begin | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | enquiries. The possible Match<br><br>The risk here is no more prevalent than in current police practices when interrogating police indices and Investigators should make all reasonable enquiries to corroborate any potential matches based on the information presented to them. | | |
| | As a result of the wide-ranging capability of RFR to process biometric data from CCTV images there is a risk that the processing of personal data may be excessive leading to regulatory action. | M | H | H | RFR can only be requested in response to an incident or investigation which provides the RFR Operator with sufficient information to determine if use is proportionate to the policing purpose for which it is intended. This also includes identifying Subjects within Probe Images or Video in order that the cropping tool can be utilised in order to | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | minimise collateral intrusion.<br><br>If the RFR Operator is not satisfied that less intrusive means have been exhausted or wouldn't provide an identification, they will not process the image or video. | | |
| | As a result of the delay in updating the Image Reference Database there is a risk that some vulnerable individuals may not be identified leading to increased harm | L | H | M | The latency between Image Reference Databases and source systems has been reduced to ten minutes which will significantly reduce the opportunity for missed images | L | |
| | As a result of potential incomplete deletion exercises there is a risk that Image Reference Databases 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 intervention and potentially cause unwarranted and unjustified damage and distress to individuals. | M | H | H | Image Reference Databases will include accurate, verifiable images lawfully held or obtained by the police for a law enforcement purpose at the time of use. No interventions will be made without checks being made on Possible Matches without manual intervention to reduce any damage and distress. SWP/GWP are | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | actively engaged with the Niche RMS supplier to develop automated deletion of non-convicted custody images. They are also an active participant of the NPCC Records Management working group which have been set up to lead on a national solution. SWP/GWP have also advertised within all custody suites the process for non-convicted image deletion requests and this information is published on the SWP/GWP websites under the privacy notice section | | |
| | 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 | L | M | M | The force will have in place appropriate policy documents for RFR for processing under Part 2 and Part 3 of the Data Protection Act 2018 | L | |
| | As a result of lack of training and awareness there is a risk the data entered onto the Image Reference Databases is not treated within the correct Government Protective Marking Scheme (GPMS) resulting | L | H | M | All SWP/GWP staff/ officers are trained in respect of the GPMS. Image Reference Databases are automatically | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | in adequate protection when handled and potential loss and damage | | | | complied in a secure environment to which the public do not have access. | | |
| | As a result of technical failure there is a risk that the equipment will not function correctly resulting in incorrect returns or failure to identify Possible Matches resulting in potential damage and distress or threat risk and harm to others | L | H | M | Officers/Staff involved in RFR do not have ready access to the complete Image Reference Databases. Operators and are briefed in respect of Image Reference Database image circulation and have been informed that this sensitive data must not be disclosed outside the operational command team, Police Officers and Staff involved in the investigation of incidents or offences, and technical support staff.<br>Those with roles specific to the oversight, operational use or management of RFR systems or record management databases. Any action following use of RFR may involve SWP/GWP working with other police | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | forces, law enforcement bodies and other agencies to assist SWP/GWP in discharging its common law policing powers. This action will not require the sharing of biometric data but may require SWP/GWP to share personal data, as it would for any investigation, in accordance with SWP/GWP's routine sharing arrangements. Physical and technical security measures are in place (as described in this DPIA) to protect RFR | | |
| | If multiple individuals are captured in the Probe Image, there is a risk their personal information will be processed during the image capture leading to excessive and unnecessary processing | L | L | L | 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. All relevant information is logged for audit purposes. SWP/GWP RFR Documents also outline points relating to RFR to | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | ensure that it is used in a way that maximises its effectiveness. The ongoing effectiveness of SWP/GWP's use of RFR will be reviewed by the FRT and Biometrics Board and the SRO. This will help ensure that any future RFR use will reflect learning identified and that the use of RFR remains an effective and proportionate policing tool<br><br>When submitting Probe Images or Video for RFR comparison, Investigators are given training to submit images containing only the Subject, or to identify the Subject in order that the cropping tool can be utilised effectively by the RFR Operator. If a video is submitted as the Probe Image, Investigators are requested to ensure the video submitted is the 'best footage' | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | of the Subject to promote identification, and to minimise the amount of video submitted for the purposes of processing the least amount of video, and ideally where no persons not involved in the investigation are present. | | |
| | The use of RFR may lead the general public to perceive that RFR is being used disproportionality towards persons from ethnic backgrounds which may lead to legal challenge, complaints and potential enforcement action | M | H | H | SWP/ GWP are conscious of the concerns raised previously in relation to bias within FRT and system accuracy relating to members of minority communities. SWP/ GWP have undertaken independent testing via the National Physical Laboratory to determine if there was evidence of bias in the way we use FRT and RFR was found to have no identifiable evidence of bias in its operation. SWP/ GWP continue to monitor the results from RFR to ensure we continue to meet our obligations to | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | ensure the technology is fit for purpose.<br><br>RFR is a post event response and is only utilised where a Subject is identified as having suspected involvement in the incident that is being investigated. There must be a policing purpose to justify the necessity to identify the Subject and any Match created is not a direction to act by the Investigator. It is necessary for the Investigator to be able to justify their actions in line with Codes of Ethics. | | |
| | There is a risk that the capability of RFR is used for non-policing purposes and function creep such as covert tactics leading to unlawful processing resulting in complaints, loss of trust and confidence, enforcement action | H | H | H | An audit trail is maintained to monitor use and prevent function creep.<br>The use of RFR must have a policing purpose, be necessary and must be considered alongside less intrusive means to be justified.<br>SWP/ GWP monitors requests for RFR and | L | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | matches to determine that necessity is made out and that requests are reasonable. Where an RFR Operator does not believe that a request is necessary or linked to a policing purpose, they will not undertake the RFR comparison. | | |
| **R10**<br>**IT Health Check**<br><br>(where an ITHC has been undertaken and the overall level of risk has been identified | | | | | | | |

## Step 6: Sign off and record outcomes

| Action | Name, position, date | Notes |
|---|---|---|
| Measures approved by: | Inspector Ben Gwyer 5369<br>Project Lead | Actions must be integrated back into the project plan with completion dates and action owners. |
| Residual Risks approved by | Inspector Ben Gwyer 5369<br>Project Lead | If accepting residual high risks, refer to DPO to consider ICO consultation before proceeding.<br>Risks should be carried over to local risk registers when processing becomes business as usual. |
| DPO advice provided | Louise Voisey<br>Data Protection Officer<br>19/08/2025 | DPO to advise on compliance, mitigating measures and whether processing can proceed |
| Summary of DPO advice:<br>I am content that this processing is compliant with Data Protection and Human Rights legislation. The framework for biometric matching is clear with suitable documentation and transparency which is reasonable. If the process or reasons for processing changes this DPIA must be revisited to identify and address any new risks. | | |
| DPO advice accepted or overruled by: | Accepted by Assistant Chief Constable Simon Belcher<br>27/11/2025 | If overruled, an explanation must be provided. |
| Comments: | | |
| Consultation responses reviewed by: | Inspector Ben Gwyer 5369<br>Project Lead | If the decision does not align with the views of the consultees please explain |

| | | |
|---|---|---|
| Comments: | | |
| Force Information Security advice: | Geraint Morgan<br>*Force Information Security Officer* | FISO to advise on security risks, mitigating measures and whether processing can proceed |
| FISO advice accepted or overruled by: | Accepted by Assistant Chief Constable Simon Belcher 27/11/2025 | If overruled an explanation must be provided |

**This is a living document and must be updated where any changes to the details provided occur.**

**Annex A - Statement of Information Assurance Requirements for External Cloud Services Provider**

The following table details the security considerations that should be considered as part of the process for procuring cloud services. Whilst all may not be applicable, they should at least be considered and comments should be made as to why they were not considered applicable.

**1. Security Requirements**

Access to the system and the data needs to be understood. If the following are required, appropriate access controls must be in place. Details should be given as to the type of controls:

| Mandatory, Desirable | Requirement | Comments |
|---|---|---|
| M | **System administrator**<br>This level must allow full access to the system, being able to undertake any part of the application including system setup.<br>Please state both your admin access and your customer's (our) admin access.<br>This should include identity and authentication controls.<br>(NSCS Cloud Security Principle 10/12) | |
| M | **Nominated user**<br>This must be a generic user with access to all major functionality, but no access to system setup. The system administrator should be able to monitor all activity generated by this user.<br>This should include identity and authentication controls.<br>(NSCS Cloud Security Principle 10/3) | |

| Mandatory, Desirable | Requirement | Comments |
|---|---|---|
| M | **User defined**<br>This could be a user with specific rights as deemed fit by the system administrator.<br>(NSCS Cloud Security Principle 10/3) | |

## 2. Further security considerations

| | | |
|---|---|---|
| M | **Compliance with HMG Security Policy Framework (SPF), ISO / IEC 27001/Cyber Essentials Plus**<br>If ISO compliant, give details as to what areas are compliant.<br>Provide copies of all relevant current certifications.<br>(NSCS Cloud Security Principle 4) | |
| M | **Information Security Policy**<br>Please include a copy of your existing security policy document(s).<br>(NSCS Cloud Security Principle 4) | |
| M | **Patching and system updates**<br>The supplier must describe its current patching and updates processes for its IT systems, including patching frequency for both routine and critical patches.<br>(NSCS Cloud Security Principle 5) | |
| M | **Data Protection Act 2018**<br>How do you comply with the Data Protection Act 2018 (including GDPR) and uphold the eight principles of good practice.<br>(NSCS Cloud Security Principle 4) | |

| | | |
|---|---|---|
| M | **Physical, Procedural, Personnel and Technical Security Measures**<br><br>The supplier must ensure there is adequate physical, procedural, personnel and technical security controls in place to prevent unauthorised access and dissemination of information assets.<br><br>Please provide appropriate documentation that evidences this (such as Statement of Intent).<br><br>(NSCS Cloud Security Principle 4) | |
| M | **Equipment Siting and Protection and storage**<br><br>Please describe the location of any hosted environment and the virtual infrastructure. Include the hardware specification, operating software and number of shared services. If a cloud based service it must comply with Police Approved Security Facility (PASF)<br><br>(NSCS Cloud Security Principle 2) | |
| M | **Data at rest and data in transit**<br><br>Please provide details on how you would protect data both at rest and in transit, including the level of encryption that would be deployed.<br><br>(NSCS Cloud Security Principle 1/2) | |
| M | **Screening**<br><br>The supplier must apply the requirements of the Baseline Personnel Security Standard (BPSS) to all personnel (incl. third party contractors) prior to giving system access to assets holding police data.<br><br>(NSCS Cloud Security Principle 6) | |

| | | |
|---|---|---|
| D | **Independent review of Information Security**<br>Do you have your site/service independently tested or audited? If so, please give details.<br>The force will reserve the rights to perform an IT Security Assessment/audit at any time. | |
| M | **Control against malicious code**<br>The supplier must ensure there are appropriate policies to manage risks from malicious code according to the impact level of the system/data which are developed and implemented.<br>Please describe what is in place to mitigate this risk.<br>(NSCS Cloud Security Principle 5) | |
| M | **Operational security**<br>The supplier must have the process to manage the service securely such as to impede, detect or prevent attacks. This should include configuration and change management, vulnerability management, a form of protective monitoring.<br>(NSCS Cloud Security Principle 5) | |
| M | **Segregation in networks**<br>There must be adequate network segregation between the police information assets and third party assets – this can be physical or virtual.<br>Please provide details of the segregation in place (computer, storage and networking components).<br>(NSCS Cloud Security Principle 3) | |

| | | |
|---|---|---|
| M | **External interfaces**<br>The supplier must provide a clear overview (diagram/description) of the information flows, which must include external interfaces (physical and logical) and how access to customer data is controlled.<br>(NSCS Cloud Security Principle 11) | |
| M | **Backup data**<br>Backup data must be kept in secure storage and location that is physically separate from the system being backed up and to which access is strictly controlled.<br>Mirrored systems should be fully tested on an annual basis to ensure that full data sets can be restored, applications can be accessed and that failover routines are effective.<br>(NSCS Cloud Security Principle 2) | |
| M | **Adequate logging of access and activity, and appropriate protection of log data**<br>Appropriate logging and auditing must be in place and that this data must be secured in such a way that tampering would be evident, for example by using the check-sum algorithm. Audit logs should be kept securely for a minimum of 12 months.<br>(NSCS Cloud Security Principle 13) | |

| | | |
|---|---|---|
| M | **Penetration Testing**<br><br>To help provide assurances about the robustness of the system/service being procured, evidence should be given of any pentation testing that has been undertaken.<br><br>It should also be expected that the force will conduct independent penetration testing of the system/service being procured prior to being accepted into service. If, as a result of this testing, vulnerabilities are identified by the pen-testing company, appropriate mitigation must be applied to the system/service provide, at their own expense, prior to implementation. | |
| M | **Reporting Information Security Events**<br><br>A robust incident management system must be in place and all relevant information security incidents must be reported to the force Information Security Team within 24 hours.<br><br>(NSCS Cloud Security Principle 5) | |
| M | **Secure disposal or re-use of equipment by supplier**<br><br>When no longer required for its original purpose equipment containing sensitive information must be stored securely until it can be disposed of in line with current government guidelines and as agreed by the force.<br><br>(NSCS Cloud Security Principle 2) | |

**3. Support and Maintenance**

It should be made clear how the system/service will be supported, including whether the support will be remote or onsite.

| Mandatory Desirable | Requirement | Comments |
|---|---|---|
| M | **Faults rectification**<br><br>Detail how support is provided. If remote, how is that expected to be achieved and what security controls are in place to protect Force data?<br><br>(NSCS Cloud Security Principle 9) | |
| D | **Upgrading**<br><br>State the policy towards upgrading and implementing new software, including the frequency of any upgrades. This should include details of how upgrades are implemented (i.e. notice given to customer and whether it is at cost?) and whether they are mandatory to stay in support.<br><br>(NSCS Cloud Security Principle 7) | |
| D | **Secure Development**<br><br>Describe how the service development (upgrades) manages new and evolving threats.<br><br>(NSCS Cloud Security Principle 7) | |
| M | **Supply Chain**<br><br>Describe support provided by your 3rd parties and how supply chain security is managed<br><br>(NSCS Cloud Security Principle 8) | |

| Mandatory Desirable | Requirement | Comments |
|---|---|---|
| D | **Secure use of the Service**<br><br>Will clear guidance be given on how the customer (the force) is expected to use the service to maintain the secure controls in place (i.e. education of users, recommended configuration etc)?<br><br>(NSCS Cloud Security Principle 14) | |

**4. Back up and resilience**

Appropriate description and evidence should be given on how the system/service will protect Force data should it be subject to a major failure. This should include details on how CIA will be maintained.

| Mandatory Desirable | Requirement | Comments |
|---|---|---|
| M | **Business Continuity**<br><br>Give details of your Business Continuity Plan (BCP), including how system/service continuity will be maintained in the event of a major failure.<br><br>(NSCS Cloud Security Principle 2) | |
| M | **Protecting the data**<br><br>The system/service must have full back-up and restore capabilities in the event of recovery from hardware or software failure.<br><br>(NSCS Cloud Security Principle 2) | |

**5. Data Retention and Disposal**

As part of the information life cycle, consideration should be given on how long the data will be held and how it will be disposed of once the contract expires.

| Mandatory Desirable | Requirement | Comments |
|---|---|---|
| M | **Archiving (if required)**<br>The supplier must state whether there is the ability to archive after a specified period and whether this is an automated process.<br>Please state if this is an additional cost.<br>(NSCS Cloud Security Principle 2) | |
| M | **Data retention**<br>The system/service must support the Forces' requirement to adhere to the Management of Police Information (MOPI) and relevant<br>Legislation/regulations (such as Data Protection Act and GDPR). Explain the proposed data retention policy that will be in place. | |
| M | **End of life strategy**<br>Please give details of what happens to Force data once the contract has ended (i.e. deletion or returned to owner?). Data returned must be in a format agreed by the force.<br>Details should include any transitory arrangements that might be put in place, along with a costing model. | |
| **Name** | | |
| **Position** | | |
| **Company** | | |

| | | | | | |
|---|---|---|---|---|---|
| **Date** | | **Telephone** | | **Email** | |

## Annex B Risk Assessment Matrix

| Risk Matrix | Likelihood | Rare | Unlikely | Possibly | Likely | Almost Certain |
|---|---|---|---|---|---|---|
| Impact | Multiplier | 1 | 2 | 3 | 4 | 5 |
| Insignificant | 1 | 1 | 2 | 3 | 4 | 5 |
| Minor | 2 | 2 | 4 | 6 | 8 | 10 |
| Moderate | 3 | 3 | 6 | 9 | 12 | 15 |
| Major | 4 | 4 | 8 | 12 | 16 | 20 |
| Critical | 5 | 5 | 10 | 15 | 20 | 25 |

Recording in Step 5

| |
|---|
| Low (L) 1-4 |
| Medium (M) 5-12 |
| High (H) 15-25 |

| Impact Definitions Table | | Value | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| EXPLANATION | **Impact on reputation** | Likely to reduce an individual citizen's perception of SWP | Likely to reduce the perception of SWP by many citizens | Likely to result in undermined confidence in SWP at a regional level. Regional press involvement | Likely to result in undermined confidence in SWP at a national level. National press involvement | May lead to a complete breakdown in public trust.<br>Ministerial involvement |
| | **Impact on privacy and identity** | Loss of control of a single persons data would cause inconvenience to them | Loss of control of many citizens' personal data beyond those authorised by each.<br>Possible requirement to report to ICO | Loss of control of a citizen's sensitive data. A compromise to the identity or financial status of an individual.<br>Possible enforcement action by ICO | Loss of control of many citizens' sensitive or financially significant personal data. Compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack Possible fine by ICO up to £0.5m | Widespread compromise of identity management systems or financial systems across SWP.<br>Prosecution by ICO and report to Parliament |
| | **Impact on life and safety** | Inconvenience or cause discomfort to an individual | Risk to an individual's personal safety or liberty | Risk to a group of individuals safety or liberty. | Threaten life directly leading to limited loss of life | Lead directly to widespread loss of life |
| | **Impact on provision of emergency services** | Minor disruption to service activities that requires reprioritisation at the local level to meet expected levels of service | Minor disruption to emergency service activities that requires reprioritisation at the area or divisional level to meet expected levels of service | Disruption to emergency service activities that requires reprioritisation at the county or organisational level to meet expected levels of service | Disruption to emergency service activities that requires reprioritisation at the national level (e.g. one police force requesting help from another) to meet expected levels of service | Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency services) to meet expected levels of service |
| | **Impact on crime fighting** | Hinder the detection, impede the investigation, or facilitate the commission of low-level crime (i.e. crime not defined in legislation as "serious crime"), or hinder the detection of serious crime | Hinder the detection, impede the investigation, or facilitate the commission of a crime (defined in legislation) | Impede the investigation of, or facilitate the commission of serious crime (as defined in legislation) | Cause major, long-term impairment to the ability to investigate serious crime (as defined in legislation) | Cause major, long-term impairment to the ability to investigate serious organised crime (as defined in legislation). |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Impact on judicial proceedings** | Minor failure in local Magistrates courts | Cause a low-level criminal prosecution to collapse; cause a conviction for a low- level criminal offence to be declared unsafe or referred for appeal. | Cause a serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred for appeal | Cause a number of criminal convictions to be declared unsafe or referred to appeal (e.g. through persistent and undetected compromise of an evidence-handling system) | Major long-term damage to UK judicial system |