South Wales Police / Gwent Police
Policy Document for the use of Retrospective Facial Recognition Technology (RFR)

Protective marking:	Official
Publication scheme Y/N:	No
Title:	Policy Document for the use of Retrospective Facial Recognition Technology (RFR)
Version:	Version 0.4
Summary:	Guidance for South Wales Police (SWP) and Gwent Police (GWP) Use of Retrospective Facial Recognition (RFR) Technology.
Branch:	Digital Services Division (DSD)
Review date:	29/06/2026

Table of Contents

Terms & Definitions: Capitalised terms used within this RFR Guidance Document shall have the meaning given to them in section 3 of this document unless otherwise defined.

1. Change Control

Change control:

Version	Date	Authority	Evidence of approval	Record of change
0.1	13/06/22	Project Lead	Inspector Ben Gwyer	Initial Draft
0.2	16/11/22	Project Oversight	Chief Insp Scott Lloyd	Amendments
0.3	09/05/23	Project Lead	Inspector Ben Gwyer	Amendments to incorporate PSED Study findings
0.4	28/04/25	Project Lead	Inspector Ben Gwyer	

2. Introduction, Aim and Scope

Introduction

2.1 Retrospective Facial Recognition (RFR) technology helps South Wales Police (SWP) and Gwent Police (GWP) identify people who are suspects for criminal offences, vulnerable and of key interest to an investigation. It helps us keep South Wales and Gwent safe. More detail about how RFR works and how SWP/ GWP uses RFR can be found in section 3 (RFR Overview).

2.2 This RFR Guidance Document provides SWP/GWP personnel with advice on the use of RFR in a legally complaint and ethical manner to enable SWP/GWP to achieve legitimate policing aims.

Aim & Scope

2.3 This guidance aims to: -

a) provide SWP/GWP personnel and members of the public with information about SWP/ GWP's present strategic, operational and technology objectives for the use of RFR, such that it enables SWP/GWP to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives); and

b) provide SWP/GWP personnel with guidance on the use of RFR technology by SWP/GWP in order to meet SWP/GWP's objectives for RFR; and

c) establish the governance structure for the use of RFR, ensuring that SWP/GWP's use of RFR is appropriately governed and legally compliant; and

d) provide an overview of RFR technology and advise on practical issues such as image quality and method of submission that impacts the Facial Recognition Technology (FRT) system.

Not in Scope

2.4 There are other forms of facial recognition (FR) that are not subject of this guidance. This includes `Live Facial Recognition' (LFR). LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist in order to locate persons of interest by generating an alert when a possible match is found. It does not include 'Operator initiated Facial Recognition' (OIFR). OIFR is a mobile phone use of FRT technology,

which compares a photograph of a person's face taken on a mobile phone to the predetermined watchlist to assist an officer to identify a subject.

2.5 In summary, this guidance does not extend to: -

a) the real-time searching of facial images from a video stream, against a Watchlist (LFR)

b) OIFR search submitted from a mobile device in near real-time; or

c) any SWP/GWP use of third-party RFR systems, or data sharing for the purpose of facilitating the use of those systems. In such instances, additional privacy considerations would be required (e.g., additional Information Sharing Agreements and audit requirements), which are beyond the scope of this guidance; or

d) the Legal Framework that is applicable to SWP/GWP's use of RFR– this is separately detailed within SWP/GWP Legal Mandate document.

Additional Documents

2.6 A number of documents are available to supplement this guidance, and these include the: -

a) SWP/GWP RFR Standard Operating Procedure (SOP)

b) SWP/GWP RFR Data Protection Impact Assessment (DPIA)

c) SWP/GWP RFR Legal Mandate

d) SWP/GWP RFR Appropriate Policy Documents

e) SWP/GWP FRT Equality Impact Assessment

f) SWP/GWP RFR Training Documents and User Guides.

3. Terminology

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

Adjudication	A human assessment of a potential match generated by the RFR application by an RFR Operator. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors.
Biometric Template	A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm and new templates will need to be generated from the original images if the Facial Recognition Technology (FRT) algorithm is changed.
Candidate Image	Image of a person in the Reference Image Database.
Environmental Factor	They are external elements that affect RFR performance such as dim lighting, glare, rain, mist etc.
Facial Recognition Technology (FRT) System Engineer	A person who is deemed to have suitable technical qualifications and experience to optimise and maintain the operational capability of the FRT System.
Facial Recognition (FR) –	The technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database generating probable matches. This is based on digital images (still or from live camera feeds)
Image Reference Database	A set of lawfully held known Candidate Images which a Probe is searched. For example, a police force's custody image database.
Match	A match occurs when the Operator, on viewing the Possible Matches, forms the belief that the Subject is identifiable as the same person shown in the Candidate Image.
No Match	The Operator determines as a result of viewing the Candidate Images and/or Possible Matches that the individual has not been successfully identified.

Probe Image	The facial image or footage submitted for a facial search against the SWP / GWP Image Reference Database.
Possible Match	Operator considers a Candidate Image may be the same person as in the Probe Image resulting in police indices being further searched.
Retrospective Facial Recognition (RFR)	Is a 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.
RFR Operator	An officer or staff member, who is responsible for establishing the legal basis for using RFR and considering Candidate Images for Possible Matches.
Similarity Score	This is a numerical value indicating the extent of similarity between the Probe and Candidate Image, with a higher score indicating greater points of similarity.
Subject	The individual whose Probe Image is considered for comparison via RFR.
Subject Factor	A factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.
SWP/GWP RFR Documents	SWP/GWP RFR Documents that regulate SWP/GWP use of RFR
System Factor	A factor relating to the FRT System such as the algorithm.
Urgency	In the context of utilising RFR, an Out of Hours request that is related to an: • Imminent threat-to-life or serious harm situation; and/or • Intelligence/investigative opportunities with limited time to act, where the seriousness and potential benefits support the urgency of action.
Out of Hours	Any time outside normal business hours 0700 - 2200

4. RFR Overview

RFR in a Law Enforcement Context

4.1 RFR technology is an operational tactic that helps SWP/GWP identify people who are wanted for criminal offences and helps protect the most vulnerable in our society.

4.2 RFR is a process in which an Investigator can submit a Probe Image or Video, whether this is obtained from Close Circuit Television (CCTV), a still image or moving video for comparison against the Image Reference Database. An RFR Operator will assess whether a Probe Image is suitable for RFR comparison and if they are satisfied, the Probe Image will then be compared against Candidate Images contained within the Image Reference Database to identify a Possible Match.

4.3 RFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against Candidate Images in the Image Reference Database in order to identify Possible Matches against an individual for a policing purpose. These Possible Matches are reviewed by an RFR Operator who then makes a decision as to the closeness of the matches and returns the Possible Match to the Investigator to consider against all other information and evidence available. The Investigator will determine the further enquiries or actions that need to be undertaken. In this way, RFR works to assist SWP/GWP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input.

RFR and SWP/GWP

4.4 RFR has been used by SWP since 2017 and in GWP since 2021. SWP/GWP believes that RFR is a valuable policing tool that helps SWP/GWP keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.

4.5 The following are illustrative examples where RFR may assist SWP/GWP with its policing purposes:

a) Supporting identification and arrest of people wanted for 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, when acting on behalf the coroner

4.6 Whilst appropriate use of RFR offers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of RFR involves biometric processing. SWP/ GWP is conscious that the use of FRT has been the subject of much debate. The areas subject of particular debate and scrutiny relate to the intrusion into civil liberties relating to the accuracy of FRT, the potential for wide-scale monitoring through the use of FRT, and the possibility for automated decision making as a result of FRT processing.

4.7 It is therefore incumbent on SWP/GWP to ensure that RFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of RFR.

4.8 In seeking to address other potential concerns, SWP has facilitated academic research and has proactively engaged with civil liberty interest groups and South Wales/Gwent Police Crime Commissioners (PCC's) Office.

4.9 SWP/GWP has listened carefully to many parties with an interest in the use of RFR and has carefully considered what safeguards are necessary to support the use of RFR. Each use must be carefully undertaken, by a trained Operator and have documented results.

4.10 The RFR Operator must also consider how the use of the technology may impact on communities, and how the rights of everyone whose image may be captured have been considered, and what safeguards are in place to protect them.

4.11 SWP/GWP is not only concerned with developing and implementing policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as RFR, are monitored for impact. SWP/GWP will implement a robust governance process to review the effectiveness and impact of RFR on an ongoing basis. SWP/GWP will focus on transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from communities as part of an ongoing process.

4.12 This Guidance document will continue to evolve to reflect changes in Legislation, Regulation, technology, and accepted use.

5. Strategic Intention, Objectives and Use Case

5.1 The use of RFR will comply with the following strategic intentions and operational objectives.

Strategic Intentions

5.2 SWP/GWP will: -

a) use RFR technology in a responsible way to identify offenders in accordance with SWP's/GWP's common law policing powers. This includes identifying those wanted for imprisonable offences, with a focus on serious crime, with a particular regard to knife and gun crime, child sexual exploitation and terrorism; and

b) strengthen and develop RFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep South Wales and Gwent Safe.

c) build public trust and confidence in the development, management and use of RFR by taking account of privacy concerns and maximising transparency; and

d) maintain good governance through an operating structure that incorporates operational and technical leads for the use of RFR, with clear decision making and accountability; and

e) ensure that the use of RFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Biometrics and Surveillance Camera Commissioner (BSCC), the Information Commissioner (ICO) and SWP/GWP RFR documents; and

f) transparently identify, manage and mitigate reputational and organisational risk to SWP / GWP; and

g) be recognised as a responsible, exemplary and ethical organisation.

Operational Objectives

5.3 SWP/GWP will: -

a) use RFR technology to enable SWP/GWP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities such as violent crime. RFR technology will increase intelligence-led enforcement opportunities including those relating to knife and gun crime, child sexual abuse, terrorism, and helping to safeguard vulnerable persons.

b) adopt a robust and proportionate approach in identifying individuals utilising an Image Reference Database, using human decision-making. Officer oversight is active and involved, with the investigating officer retaining responsibility for quality assuring Matches, making reasonable enquiries to corroborate that Match with evidence and retaining responsibility for decisions to take further action based upon evidence available

c) engage with and provide reassurance to communities, listening and responding to concerns; and

d) continually identify and review risks relevant to the RFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

Technological Objectives

5.4 SWP/ GWP will: -

a) ensure all RFR technology is fit-for-purpose and utilised effectively in line with strategic intentions and operational objectives; and

b) provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other imprisonable offences; and

a) look to technological improvements whilst keeping SWP/ GWP model under review. Where appropriate we will trial alternative providers of facial recognition software and hardware in parallel with our current provision. This helps to ensure that the best possible service is sought, and we can proactively develop improved working methodologies and accuracy. The outcomes of any parallel trial will be captured with the same key performance metrics that are gathered when utilising RFR to ensure the findings are suitable for direct comparison and analysis. All previously detailed retention periods will remain unaffected. Personal information that is processed in this manner will not be shared with any third-party individual.

6. Overview of RFR Processes

End-to-End Process

5.1 The standard end-to-end process of an RFR use can be summarised as follows: -

a) Submission is made via a Niche workflow, secure email, evidence management system or encrypted USB drive to the SWP Identification (ID) unit.

b) The RFR Operator will ensure they are satisfied there is a law enforcement purpose identified, safeguards are considered, and the correct Image Reference Database identified.

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 Probe 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.

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.

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)

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.

g) Any result is then passed to the investigating officer via a Niche workflow.

h) A record of the search and the outcome is recorded by the RFR Operator.

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.

5.2 SWP/GWP Standard Operating Procedure (SOP) provides a greater level of detail about the processes involved in the use of RFR by SWP/GWP.

Key Points

a) RFR uses images of people captured from a variety of sources including but not limited to public & private CCTV, witnesses personal electronic devices and officers Body Worn Video.

b) The angle at which the original image is captured is critical to capturing a suitable Probe Image;

c) The quality and resolution of images (both those in the Image Reference Database and the Probe Images) are of vital importance and must be carefully considered;

7. Governance, Oversight and Impact Assessments

Governance Framework

7.1 SWP/GWP RFR Documents address the stipulations detailed above. 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.

Pre-Operational Use

7.2 The initial request to undertake an RFR comparison 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.

7.3 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. For requests received outside of Niche this information will be recorded locally in a secure database.

7.8 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: o Common law policing powers o Human Rights Act 1998 o Equality Act 2010 o Protection of Freedoms Act 2012 o Data Protection Act 2018 • 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 • Data retention periods applicable to RFR
SWP/GWP RFR Standard Operating Procedure (SOP)	• Outlines measures relevant to considering when RFR can be used by SWP/GWP. • Reference Image Database considerations including the basis on which images may be added to an Image Reference Database.
SWP/GWP RFR Data Protection Impact Assessment (DPIA)	• Describes the nature, scope, context and purposes of the processing. • Assesses necessity, proportionality and compliance measures. • Identifies and assesses risk to individuals. • Identifies any additional measures to mitigate those risks.
SWP/GWP RFR Appropriate Policy Documents	• Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the Data Protection Act (DPA) 2018. • Explains how the processing of special category data under Part 2 DPA 2018 and Article 9 General Data Protection Regulation • Explains how SWP/GWP complies with the Law Enforcement data protection principles and the GDPR principles. Outlines policies as regards the retention and erasures of personal data.
SWP/GWP FRT Equality Impact Assessment	• Promotes all aspects of equality. • Ensures compliance with the law, taking into account of equality and human rights.

Operational Use

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

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

Post-Use

7.11 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.

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

8. Oversight Bodies and Regulatory Framework

8.1 Within SWP/GWP, the senior internal oversight body for RFR is the FRT Programme Board, which in-turn answers to SWP/GWP Gold Board. In addition, the SWP Police and Crime Commissioner's Office (PCC) and the GWP PCC's Office also provide an external oversight and scrutiny perspective.

8.2 SWP/GWP RFR Legal Mandate sets out the legal framework for SWP/GWP use of RFR technology, whilst SWP/GWP RFR Policy Document and SWP/GWP RFR SOP support implementation.

8.3 Nationally, the 'National Police Chiefs Council (NPCC) Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.

8.4 Further oversight opportunities may arise in relation to the `National Biometrics Strategy Board' (NBSB). This is co-chaired by the NPCC lead for Biometrics and the Home Office Data and Identity Department, it is attended by representatives of the Information Commissioners Office, the Biometrics and Surveillance Camera Commissioner, and Office of the National Police Chief Scientific Adviser. More detail on these roles: -

a) Biometrics and Surveillance Camera Commissioner (BSCC); The role of the Biometrics and Surveillance Camera Commissioner is to:

- keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints.
- decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984)
- review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints
- provide reports to the Home Secretary about the carrying out of his functions
- encourage compliance with the Surveillance Camera Code of Practice
- review how the code is working
- provide advice to ministers on whether or not the code needs amending

The commissioner is independent of government. The commissioner has no enforcement or inspection powers regarding surveillance cameras and works with relevant authorities to make them aware of their duty to have regard to the code.

See About us - Biometrics and Surveillance Camera Commissioner - GOV.UK (www.gov.uk)

b) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Privacy Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

See www.gov.uk/government/organisations/information-commissioners-office.

c) National Police Chief Scientific Adviser (NPCSA); The role of the Chief Science Advisor is to provide Police Chief Officers with advice on all aspects of policy on science and technology.

See www.gov.uk/government/groups/chief-scientific-advisers

9. Public Engagement

9.1 Public engagement must be supported using online resources available to the public, which should be underpinned by press and media strategies.

9.2 Our operational use of RFR should be promoted with openness with the public and transparency about the use of RFR, to increase awareness of how RFR helps keep the public safe and how it helps bring offenders to justice.

9.3 Key stakeholders, including the PCC's, may be invited to observe the use of RFR.

10. Testing Equitability

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

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

10.3 NPL Equitability Study Methodology: To automate the testing of RFR, batch processing of identification searches using the Neoface M40 algorithm was utilised. This removed the requirement of operator involvement. The program uses the Neoface facial recognition server to perform an identification search of each probe image in a specified directory against a Image Reference Database, and logs the identifiers of the returned Candidate Images, and the corresponding comparison scores.

Image Reference Database and Probe images

The Image Reference dataset for RFR combines (i) an enrolled watchlist of Custody-style Cohort images, and (ii) the enrolled Filler dataset of custody images.
The probe images used for RFR were the full set of facial images of the Cohort subjects collected in conjunction with the LFR deployments. The image types are listed within the methodology of the NPL Equitability Study in **Error! Reference source not found.**.
For RFR, the matching process was configured to return for each probe the comparison score and candidate ID of the top 200 matches in the Image Reference Database.

10.4 The full results are presented in the National Physical Laboratory's commissioned report 'Facial Recognition Technology in Law Enforcement Equitability Study'. The full study can be accessed via:

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

What does this study tell us about accuracy of SWP's FRT?

10.5 The NPL report provides an impartial, scientifically underpinned, evidence-based robust analysis of the performance of SWP's FRT System in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.

10.6 For every probe image submitted for RFR, the correct reference was returned at Rank 1 (i.e., as the top match). This is the best possible performance[1].

10.7 It follows that TPIR is identical at 100 % for all demographic subsets of the submitted probe images and, with no demographic variation in TPIR, the performance is equitable.
The result also suggests that in the operational use of RFR, the number of top-matching candidates returned for operator adjudication could be somewhat smaller than 200 (say 10 rather than 200).

Did the study find any differences in SWP's FRT?

10.8 For all demographic sub-groups, there was no variation, and performance of RFR is equitable

10.9 Reflective of the need for continuous improvement, SWP will continue to monitor its FRT performance, in terms of both overall system accuracy and demographic differential performance going forward.

11. Dataset Considerations

Image Quality

11.1 The performance of the FRT System is heavily dependent on the quality of the images in the Image Reference Database. The best images are those that follow a custody or passport style image that conforms to the National Policing Improvement Agency (NPIA) 'Police Standard for Still Digital

Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'. Further detail are included within the embedded PDF:

NPIA Standard Still Digital Images.pdf

11.2 Where multiple images of a Subject are available, these will be included in the Image Reference Database where it is advised that they will improve the likelihood of identifying those of interest to SWP/GWP.

Addressing Disproportionality

11.3 SWP does not create or retain a breakdown of race, gender or any other protected characteristic[2] of persons in the Image Reference Database. This mirrors the approach taken with the majority of policing tools used by SWP/GWP.

11.4 The routine retention of data relating to protected characteristics would mean SWP/ GWP holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals within the Reference Image Database.

11.5 SWP/ GWP also carries out bias testing of the FRT System when necessary. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

11.6 SWP/ GWP has a number of measures to guard against a System Factor (system bias) affecting the generation of Potential Matches.

These measures include that: -

a) those involved in RFR use monitor Potential Matches, Subject Factors and System Factors during use. Should concerns arise that the FRT System is not performing correctly the RFR Operator will inform a supervisor immediately.

b) for the purpose of facilitating post-use reviews, Possible Matches are retained. It provides further opportunity to consider the Subject, System and Environmental Factors, and the effectiveness of the safeguards in place for the Use.

12. Key Performance Metrics

12.1 This section covers some of the key performance metrics that should be gathered when utilising RFR. It outlines the minimum requirements and so additional metric, or indicators may well be relevant and suitable for collation and analysis. The key performance metrics will be reported to monthly project meetings to provide oversight at NPCC level.

[2] As defined in Section 4 of the Equality Act 2010.

12.2 Total Submissions. The quantity of Probe Images and Videos submitted for RFR analysis on a monthly basis.

12.3 Total suitable submissions. The quantity of Probe Images and Videos submitted that were of a suitable quality for RFR analysis.

12.4 Total submissions not suitable for RFR analysis. The quantity of Probe Images or Videos that are not suitable for analysis. This could be for a variety of reasons including the angle of image capture and other environmental factors

12.5 Matches. The number of Matches passed to officers to progress an enquiry.

12.6 No Matches. The number of No Matches returned to the Investigating Officers.

13. RFR Guidance Summary

13.1 This guidance relates to the operational use of RFR, and the governance and oversight regimes necessary to support Use.

13.2 It is strongly advised that officers and staff adhere to the guidance as this will help ensure that SWP/ GWP use of RFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.

13.3 It is recognised circumstances may arise where for valid reasons, a decision is taken that it is necessary to operate outside of this guidance. This guidance will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are at odds with some aspects of this guidance, it is essential these decisions are fully documented, together with detailed rationale, and that the relevant decision-making features within debrief and evaluation processes.

14. Data Retention & Data Management

14.1 SWP/ GWP must ensure that the processing of any data associated with RFR is conducted in a lawful way and in compliance with the SWP RFR Documents.

14.2 The retention periods that apply to the FRT system, specific to RFR are:

a) Image of the Subject ('Probe Image') - MOPI retention of personal information
b) Biometric Template of Probe Image - immediately deleted in the FRT system at the conclusion of the RFR comparison.
c) Image Reference Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS
d) All outcomes of RFR comparisons are recorded on Occurrence log of the Occurrence to which they relate.

14.3 Retention periods specific to Source System (MOPI) – Niche Record Management System

Please refer to Home Office Review of the Use and Retention of Custody Images published February 2017 (recommendation 4)

Non-conviction – upon request
Group 1 or 2 (Public Protection Matters & sexual, violent or other serious offences respectively) – 10 years upon request then review
Group 3 (all other offences) – 6 years upon request then review
Group 4 (missing persons) – 6 years then review

All other personal data will be stored in accordance with MOPI standards.
Group 1 - subject is 100 years the review
Group 2 – 10 year clear period then review
Group 3 – 6 year clear period
Group 4 (missing persons) – 6 years then review

14.4 To support compliance the FRT System has a full audit capability.

14.5 Data relating to historical searches is retained no longer than is operationally necessary.

14.6 The loss or theft of any FRT hardware or other data, irrespective of whether or not protected by encryption, must be reported immediately to the SWP Data Protection Officer.