South Wales Police / Gwent Police
Standard Operating Procedure for the use of Retrospective Facial Recognition Technology (RFR)

Protective marking:	Official
Publication scheme Y/N:	No
Title:	Standard Operating Procedure (SOP) for the use of Retrospective Facial Recognition (RFR) Technology
Version:	Version 0.2
Summary:	Establishes procedures for the use of Retrospective Facial Recognition (RFR) technology in support of policing operations.
Department:	Digital Services Division (DSD)
Review date:	29/06/2023

Version	Date	Authority	Evidence of approval	Record of change
0.1	11.10.2022	Project Lead	Inspector Ben Gwyer	Initial Draft
0.2	14.09.2022	Project Oversight	Ch. Insp Scott Lloyd	Amendments
0.3	09.05.2023	Project Lead	Inspector Ben Gwyer	Amendments to incorporate PSED Study findings

Contents

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

1 Introduction

1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when using Retrospective Facial Recognition (RFR) technology in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool.

2 Application

2.1 All South Wales and Gwent police officers and police staff, including the extended police family and those working voluntarily or under contract to the Commissioners must be aware of, and are required to comply with, all relevant SWP/GWP policy and associated procedures.

2.2 This SOP applies in particular to officers and staff in the following roles: -

a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the request and use of RFR technology; and

b) All police officers and police staff involved in any subsequent investigation resulting from the use of RFR technology; and

c) RFR Operators and Facial Recognition Technology (FRT) System Engineers.

Note: This list is not intended to be exhaustive.

3 Terminology

3.1 This SOP focuses exclusively on RFR. Terminology relating to RFR is defined in the SWP/GWP RFR Policy Document.

4 Use of RFR

4.1 The Submission of images for RFR can be made by any SWP/GWP officer or member of staff however they must ensure that the purpose of the submission is identified, and all safeguards have been considered. The review of the necessity for submission will form the general duties of their supervisor.

4.3 Before any processing is undertaken, the RFR Operator:-

a) must consider the legitimate aim of the use and the legal powers that are being relied upon to support the Use; and

b) means that the RFR Operator is satisfied that the use complies with SWP/GWP RFR Documents, or is otherwise authorised; and

c) must, from a Human Rights Act 1998 perspective, understand (i) how and why the use is necessary (and not just desirable), and (ii) is proportionate to achieve the legitimate aim of the use; and

d) must, from a Data Protection Act (DPA) 2018 perspective, articulate that it is strictly necessary for the SWP's/GWP's law enforcement purposes; meaning

there is a `pressing social need' and it is not reasonably viable to address this through less intrusive means, either because less intrusive tactics have been tried, or it is reasonably believed that those tactics are unlikely to be effective; and

i. Necessary on at least one of the following grounds (the ground(s) to be confirmed by RFR Operator): -

a. Necessary for SWP's/GWP's lawful policing purposes[1] for reasons of substantial public interest; and / or

b. Necessary for the administration of justice; and / or

c. Necessary for the safeguarding of children and/or of individuals at risk; and

ii. Necessary notwithstanding any expectations people may have pursuant to their Article 8 Human Rights Act regarding the respect of private and family life, as well as other human rights considered by the RFR Operator; and

e) must understand that the RFR Operator has given regard to the safeguards proposed for the use and the safeguards contained within the SWP/GWP RFR Documents, and considers that the use in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the DPA2018; and

f) is satisfied that all reasonable steps have been taken to ensure that the composition of the Reference Image Database and Probe Image complies with SWP/GWP RFR Documents.

g) must have received SWP RFR training as per the SWP/GWP RFR Documents; and

h) considers that the use is proportionate with the benefits anticipated from the use of RFR outweighing the concerns and impacts there may be in relation to people's human rights and rights relating to equalities; and

i) is satisfied that the control measures in the Data Protection Impact Assessment (DPIA), and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the use.

5 Reference Image Database

5.1 This section covers the generation and management of the Reference Image Database to be used in RFR. The Reference Image Database for use with RFR must have a defined policing objective.

[1] This being defined as "is necessary for the exercise of a function conferred on a person by an enactment or rule of law" in the Data Protection Act 2018. This will typically be the ground relied on to support SWP uses of RFR since this recognises the policing powers conferred on a Constable.

Reference Image Database: -

a) must only contain images lawfully held by SWP/GWP; and

b) must only use images where all reasonable steps have been taken to ensure that the image is of a person intended for inclusion in the Reference Image Database.

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

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

5.4 Examples of images that may be deemed appropriate for inclusion within a Reference Image Database include: -

a) custody images of individuals

6 RFR Probe Images

6.1 This section covers the generation and management of Probe Images to be used in RFR uses. Probe Images submitted to RFR must have a defined policing objective. Probe images can be a still image provided by police, a 3rd party or an image extracted from moving video by the FRT System.

6.2 Probe Images must only contain images lawfully held by SWP/GWP and must endeavour to use images where all reasonable steps have been taken to ensure that the image is of a person intended for RFR analysis.

7 SWP RFR Documents

7.1 Assessments; For RFR USE, the following assessments need to be created, reviewed, and amended where necessary: -

(i) Data Protection Impact Assessment* (Review/Amend/Adopt); and

(ii) Equality Impact Assessment* (Review/Amend/Adopt); and

Note: *Any assessment listed above showing `Review/Amend/Adopt' has already been created by the SWP/GWP FRT team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each RFR operation.

8 Management of Risk

8.1 FRT System Engineers will be available to support RFR use as will members of the FRT Team within DSD.

8.2 All RFR Operators and staff involved in a RFR use must receive RFR training prior to use.

9 RFR Operational Roles

9.1 RFR Operators will: -

a) receive detailed training prior to using the FRT System.
b) ensure the legality and necessity of the submission of Probe Images and video.
c) review Possible Matches generated by the FRT System and determine if a Match has been made
d) Inform the submitting officer/ Officer in case of the Match
e) ensure all key performance metrics are recorded accurately.

9.2 Investigating Officer:- On receipt of a Possible Match, prior to arrest or other intervention, the Investigating Officer will:-

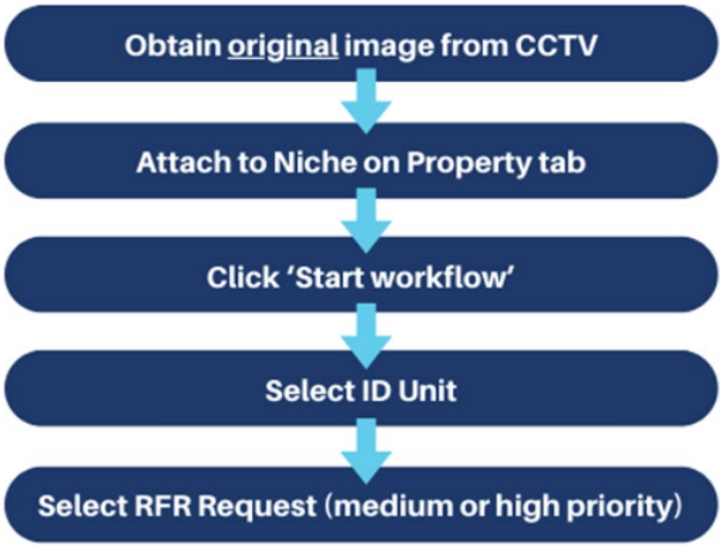
a) Review the Match to corroborate it is accurate

b) Review other evidence that has been obtained as part of the investigation for corroboration

9.3 The Investigating Officer must consider all of the evidence available and follow up all reasonable enquiries as in any normal investigation, even if these enquiries lead them away from the person identified by RFR.

9.4 The fact that a Match has been made does not replace the necessity for the Investigating Officer to form reasonable grounds to suspect the person identified is responsible for the commission of an offence and that necessity exists to justify an arrest. This is also the case in respect of consideration of whether to arrest or consider less intrusive means to achieve the requirements of the investigation (i.e. Voluntary Attendance)

10 Image Submission Process



11 Urgent Submissions

11.1 Urgent Submissions outside of the standard office hours of 0700-2200 will require authorisation from the relevant Force Incident Manager (FIM) and will be conducted by trained staff in South Wales Police Public Service Centre (SWP PSC).

12 RFR System Security

12.1 The FRT System includes a number of physical and technical security measures. These include: -

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

b) the FRT System is secured according to South Wales Police Procedures and accessed via active directory permissions.

c) role based access controls with limited user permissions are implemented on the FRT System; and

d) the Dashboard and RESTful API are secured with SSL and TLS by default; and all connections are directed through HTTPS; and

e) a full audit is maintained of all user initiated actions undertaken during the course of a use; and

f) technical issues with the FRT System are always dealt with by FRT System Engineers within SWP IT with assistance from the FRT Project team.

13 Data Retention & Data Management

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

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

13.3 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.

13.4 All uses of RFR will be recorded in a central register and an audit trail will be recorded on the relevant Niche record for that submission.

14 Contact Information

14.1 The SWP/GWP RFR team can be contacted using the following email address; FRT@South-wales.police.uk.

14.2 The ID Unit who have primacy for RFR searches are contactable on PROMAT@South-Wales.police.uk.