



Data Protection Legislation

Appropriate Policy Document (APD)

Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 Data Protection Act 2018

South Wales Police / Gwent Police Retrospective Facial Recognition (RFR)

Processing biometric data, for the purpose of uniquely identifying an individual.

September 2022

Version 1.4

Version Control

Version	Date	Author	Purpose
V1.0	09/12/2020	S.Lloyd	Original Draft
V1.1	31/12/2020	S.Lloyd	DSD SMT Review
V1.2	12/01/2021	S.Lloyd	DPO Review

V1.3	16/04/2021	S.Lloyd	FRT Board Review
V1.4	29/09/2022	S.Lloyd	Review

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

Introduction

This policy document has been produced in accordance with South Wales Police' Gwent Police' obligations under Part 3 of the Data Protection Act 2018 (DPA). It should be read alongside the South Wales Police / Gwent Police Record of Processing Activities (maintained in accordance with [Article 30 General Data Protection Regulation GDPR and section 61 DPA](#)), and the South Wales Police / Gwent Police [Privacy Notice](#). Data protection policy specific to RFR is also to be found in the RFR Policy and Data Protection Impact Assessment (DPIA) and the Part 2 DPA and Article 9 GDPR.

Sections 35(3), 35(5)(c) and 42 Part 3 of the DPA 2018 set out the requirement for an APD to be in place when conducting sensitive processing of personal data for Law Enforcement (LE) purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to GDPR special category data. Sensitive processing includes: -

- a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- c) the processing of data concerning health;
- d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. In addition, you may only process sensitive personal data for LE purposes if you have an APD, and if the processing: -

- is based on the consent of the data subject - section 35(4);

or

- is strictly necessary for the LE purpose and is based on a Schedule 8 condition - section 35(5).

This Policy Document

This document will demonstrate that the processing of this sensitive data is compliant with the requirements of Part 3 section 42 of the DPA.

Description of Data Processed

The sensitive data processed utilising RFR: -

- Biometric data for the purpose of uniquely identifying an individual.

RFR is a post event use of facial recognition technology (FRT), which compares still images of faces of unknown subjects against a Reference Image Database in order to identify them.

The Reference Image Database for RFR is the South Wales Police / Gwent Police custody image dataset.

All custody images will have a Biometric Template created (sensitive personal data) at the point of enrolment to the FRT system.

An RFR Probe Image is any facial image which is searched against the Reference Image Database and can be retrieved from a variety of sources. The common sources of RFR Probe Images may include CCTV systems, digital cameras, mobile phones and social media, although any source of image will be considered.

All faces compared against the Reference Image Database have a Biometric Template created (sensitive personal data).

Whilst utilising RFR a Probe Image is searched against every Candidate Image in the Reference Image Database.

Biometric data used to uniquely identify an individual is considered to be sensitive personal data. For this processing we will be collecting the personal data of members of the public which will include an image that may be utilised by extracting a Biometric Template from it for the purposes of uniquely identifying them. Where this data does not match that held on the reference image database it will not be further processed

and biometric data of the individual permanently deleted. No other personal identifiers are collected in addition to the Biometric Template.

South Wales Police / Gwent Police is not relying on consent for processing.

Conditions for processing sensitive data.

There are a number of relevant conditions in Schedule 8 which will apply for use of RFR, which apply to current policing practices in any event:

1. Statutory etc. purposes

This condition is met if the processing—

- (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
- (b) is necessary for reasons of substantial public interest.

The police have a common law duty to prevent and detect crime: this is the relevant 'rule of law' pursuant to which the processing is necessary for the police to exercise their functions. The processing is also necessary for reasons of substantial public interest, that is, the prevention and detection of crime and the safety of the public. In determining necessity, South Wales Police / Gwent Police will always consider whether less intrusive measures can be used without compromising the objective and the interests of the individual balanced against the interests of the community.

Condition 1 is the primary condition relied upon. However, there are other Schedule 8 conditions which may also apply:

2. Administration of justice

This condition is met if the processing is necessary for the administration of justice.

E.g. The identification of individuals who are evading justice having committed a criminal offence or who are interfering with the administration of justice

3. Protecting individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or another individual.

E.g. Where an individual is unconscious or it is necessary to assess the immediate danger to officers or other individuals by establishing if there is a known history of violence.

4. Safeguarding of children and of individuals at risk

This condition is met if-

(a) the processing is necessary for the purposes of-

- (i) protecting an individual from neglect or physical, mental or emotional harm, or
- (ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is-

- (i) aged under 18, or
- (ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

Please refer to the Data Protection Act 2018 for the full provisions of this condition.

E.g. processing of images of persons believed to be missing persons.

8. Preventing fraud

(1) This condition is met if the processing-

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of-

- (i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,
- (ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or
- (iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

E.g. processing images for persons suspected of committing a fraud offence.

Procedures for ensuring compliance with the DPA principles

Accountability Principle

South Wales Police / Gwent Police have put in place appropriate technical and organisational measures to meet the requirements of accountability and demonstrate compliance with wider requirements of Part 3 of the DPA 2018 and in particular the principles. These include: -

- The appointment of a data protection officer who is responsible for data protection compliance for RFR; who reports directly to the Chief Officer team for South Wales.
- Taking a 'data protection by design and default' approach to our activities.

- Maintaining documentation of our processing activities specifically with reference to section 61 and 62 DPA 2018.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out DPIA's for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (1): lawfulness and fairness

Processing personal data must be lawful and fair. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing is necessary for the performance of a task carried out for that purpose by South Wales Police / Gwent Police as a competent authorities. As RFR involves sensitive processing, in addition, in the absence of consent, it is only lawful if the processing is strictly necessary for the LE purpose and the processing meets at least one of the conditions in Schedule 8 and South Wales Police / Gwent Police has in place this APD.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document. The DPIA for RFR gives specific detail regarding the way in which data is processed and how the measures we have in place ensure that the processing is lawful, fair and transparent. Relevant documentation and additional information about how RFR is used is available to the public on the [Home | South Wales Police \(south-wales.police.uk\)](https://www.south-wales.police.uk).

The processing of data by RFR is strictly necessary for the exercise of South Wales Police / Gwent Police' functions of preventing and detecting crime and protecting public safety for reasons of substantial public interest (see above under **Conditions for processing sensitive data**). Reliance will be primarily on condition 1 of Schedule 8, but conditions 2, 3, 4 and/or 8 may also apply. We have given examples of where this may be the case above. South Wales Police / Gwent Police will always consider whether the use of RFR is strictly necessary (i.e. taking into account consideration of other measures not involving sensitive processing and whether they could achieve the same outcome) and will ensure that at least one relevant condition is satisfied.

Principle (2): purpose limitation

South Wales Police / Gwent Police' LE purposes for processing using RFR are primarily the prevention, investigation, detection and prosecution of crime but also the safeguarding against and the prevention of threats to public security. These are all LE purposes under s.31 DPA 2018.

On each occasion that RFR is used, the relevant specific and legitimate LE purpose will be explicitly recorded.

We process sensitive data using RFR when it is necessary for us to fulfil these statutory functions listed above in the substantial public interest, including where it is necessary for complying with or assisting another body to comply with a regulatory requirement, to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts, or for disclosure to elected representatives. An example would be if an individual is suspected of committing a criminal offence.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other LE purposes here, providing the processing is necessary and proportionate to that purpose. This means that in particular we consider what we seek to achieve, whether there are alternative measures which would not involve sensitive processing but which would achieve substantially the same outcomes, and the same or lesser impact on individuals and the community.

If we are sharing data collected for LE purposes with another controller, we will document that they are authorised by law to process the data for their LE purpose and that the processing is necessary and proportionate to that purpose.

We will not process personal data for purposes incompatible with the original purpose for which it was collected.

We will not process data collected for an LE purpose for a purpose that is not an LE purpose unless the processing is authorised by law and meets the requirements of the GDPR and DPA.

Principle (3): data minimisation

We process personal data necessary for relevant LE purposes/s and ensure it is adequate, relevant and not excessive in relation to the purpose(s) for which it is processed. The information we process is only that which is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. An example would be if another individual's image was captured that was not subject to an enquiry.

In addition, we require the data to be of an acceptable quality for comparison e.g. an image of a face with a minimum of fifty pixels between the eyes of the subject. For RFR, this is sufficient facial biometric data to compare against a Reference Image Database.

Ultimately a RFR Operator will determine whether a Match is made between the Probe and Candidate Image where the automated comparison indicates that they may be the same person. This is an additional safeguard against identification of similar but incorrect individuals.

Principle (4): accuracy

We will retain the Probe Image of the Subject and Biometric Template for no longer than is necessary for the LE purpose for which it is processed. The Probe Image will be maintained in accordance with the Management of Police Information (MOPI), the Biometric Template of the Probe Image will be automatically and immediately

deleted from the FRT System after a search is completed. The comparison process takes a matter of seconds. The RFR search reorders the database based on a Similarity Score with further consideration will be undertaken by the RFR Operator. Where we become aware that personal data contained within the Reference Image Database is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. This is an automated process and occurs every five minutes. This will involve comparing Candidate Images in the FRT system and images from the databases that have supplied them, both sets of images will have a hash value applied and compared for accuracy to ensure they are the same. If there is an imbalance an alert will be sent to the database team for review. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision and take appropriate steps to inform the data subject. Where we erase or rectify personal data we will inform any recipients with whom we have shared that data.

Principle (5): storage limitation

All sensitive data processed by us for the purpose of an LE purpose is retained for the periods set out in our retention schedule. The Probe Image will be maintained in accordance with the Management of Police Information (MOPI), the Biometric Template of the Probe Image will be automatically and immediately deleted from the FRT System after a search is completed. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (6): integrity and confidentiality (security)

Personal data processed by RFR is processed within our accredited secure computer network which is located locally within South Wales Police force area in accordance with national and local security policies. Hard copy information is processed in line with our information management policies. Data Protection Polices are applied from inception of initiatives to ensure legislative compliance with our data protection obligations and to determine appropriate levels of technical and organisational safeguards and controls when processing personal data and sensitive data. All of our security measures are designed to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

Our electronic systems and physical storage have appropriate access controls applied including for example, multi-factor authentication to access mobile devices (in the form of multiple sign in/access codes/facial recognition etc), password protection, encryption and locking mechanisms. Information Asset Owners are responsible for ensuring that all information management processes are applied to information and there is a continuous cycle of review and information risk identification and management. RFR has also been subject to a robust DPIA.

All staff receive basic data protection training must undertake annual mandatory training for managing information. Specific training is provided to officers working with RFR which is supplemented with bespoke Standard Operating Procedures

The systems we use to process personal data allow us respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information is held. All events which take place on operation systems are recorded on an audit log which enables identification of the action executed, when it was carried out and by whom.

Retention and Erasure

Particular to the FRT System

- Image of the Subject ('Probe Image') - MOPI retention of personal information
- Biometric Template of Probe Image - immediately deleted in the FRT system.
- Reference Image Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS

Source System – Niche Record Management System

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

Non-conviction – upon request

Group 1 or 2 (Public Protection Matters & sexual, violent or other serious offences respectively) – 10 years upon request then review

Group 3 (all other offences) – 6 years upon request then review

Group 4 (missing persons) – 6 years then review

All other personal data will be stored in accordance with MOPI standards.

Group 1 - subject is 100 years the review

Group 2 – 10 year clear period then review

Group 3 – 6 year clear period

Group 4 (missing persons) – 6 years then review

Appropriate Policy Document review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

Account is taken of all regulatory and policing information and guidance, relevant case law and changes to legislation.

A copy of this policy will be published on the South Wales Police website and a copy is available to the Information Commissioner, on request, free of charge in accordance with s42(3)(cc) DPA.

Further information relating to South Wales Police / Gwent Police RFR can also be found in relevant supporting documents, to include:-

- RFR Standard Operating Procedures – How to guide for officers
- RFR Policy Document
- RFR Data Protection Impact Assessment
- RFR Equality Impact Assessment
- RFR Legal Mandate

Other relevant policies/guidance documents available to police personnel are:

Information Security Information

Data Protection Policy

DPIA Guidance

Information Asset Management Guidance

Information Asset Owner Handbook

Information Risk Management Guidance

Data Minimisation, Anonymisation and Pseudonymisation Guidance

Consent Guidance

Force Retention Schedule

Policy document Sign-Off

Person completing the APD	Name (in capitals)	Scott Lloyd Chief Inspector
	Date:	31/12/2020
Data Protection Officer	Name:	Louise Voisey
	Date:	05/06/2023
Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))	Signed:	

	Name (in capitals)	Simon Belcher Chief Superintendent
	Date:	29/06/2023