HEDDLU DE CYMRU
SOUTH WALES POLICE

Appropriate Policy Document: Retrospective Facial Recognition (RFR) Part 2 Data Protection Act 2018

General Processing

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

This document is a policy for special category data and/or criminal offence data processing by the force as part of Operator Initiated Facial Recognition ("OIFR"). Where there are potentially high risks as a result of specific processing activities, a tailored policy document will be produced in respect of that activity, however this will be on an exceptional basis.

Force	SWP/ GWP
RoPA Ref:	IG/42
DPIA Ref:	AR0120
APD No.	APD003a.i.

1. Description of data processed

Give a brief description of each category of special category data/criminal offence data processed and indicate how long it is retained for.

Special Category Data *Special category data includes personal data* ***revealing or concerning*** *the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special*	Indicator "x"	Description of Data	Retention

category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.			
Data revealing race or ethnic origin			
Data revealing political opinions			
Data revealing religious or philosophical beliefs			
Data revealing trade union membership			
Genetic data			
Biometric data (where used for identification purposes)	x	RFR is a post event use of facial recognition technology (FRT), which compares still images of faces of unknown subjects against an Image Reference Database in order to identify them. The Image Reference Database for RFR is the South Wales Police / Gwent Police custody image dataset. The images in the Image Reference Database are referred to as Candidate Images. All Candidate 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 Image Reference Database and can be retrieved from a variety of sources. Common sources of Probe Images may include CCTV systems, digital cameras, mobile phones, dash cams, and doorbell cameras. The faces of individuals in the Probe Image will have a Biometric template created from the Probe Image and this	No biometric templates are retained.

		will be compared against the Image Reference Database. Whilst utilising RFR a Probe Image is searched against every Candidate Image in the selected Image Reference Database(s). At the conclusion of the comparison, regardless of whether a match has been made, the Biometric Template of the Probe Image is automatically and immediately deleted. South Wales Police / Gwent Police is not relying on consent for processing.	
Data concerning a person's sex life			
Data concerning a person's sexual orientation			

Criminal Offence Data	Indicator "x"	Description of Data
Criminal Activity	x	The Image Reference Database will contain images of individuals previous arrested by SWP/ GWP and taken into custody
Criminal Allegations (including unproven allegations)	x	As above – the subject may be on bail
Criminal Investigations	x	As above
Criminal Proceedings	x	As above
Criminal Offences	x	As above
Criminal Penalties/Sanctions/Fines	x	As above
Information about the absence of convictions		
Conditions or restrictions laced on an individual as part of the criminal justice process	x	As above
Civil Measures which may lead to a criminal penalty if not adhered to.		

2. Schedule 1 DPA 2018 Condition for Processing

Please insert link to Privacy Policy, record of processing or any other relevant documentation if appropriate:
SWP Privacy Notice

Schedule 1 conditions	Indicator "x"
Part 1 Conditions relating to Employment, Health and Research	
Employment, social security and social protection	
Health or social care purposes	
Public health	
Research etc	
Part 2 Substantial Public Interest Conditions	
Statutory etc and government purposes	x
Administration of justice and parliamentary purposes	x
Equality of opportunity or treatment	
Racial and ethnic diversity at senior levels of organisations	
Preventing or detecting unlawful acts	
Protecting the public against dishonesty etc	
Regulatory requirements relating to unlawful acts and dishonesty etc	
Journalism etc in connection with unlawful acts and dishonesty etc	
Preventing fraud	
Suspicion of terrorist financing or money laundering	
Support for individuals with a particular disability or medical condition	
Counselling etc	
Safeguarding of children and of individuals at risk	x
Safeguarding of economic well-being of certain individuals	
Insurance	
Political parties	
Elected representatives responding to requests	
Disclosure to elected representatives	
Informing elected representatives about prisoners	
Anti-doping in sport	

Standards of behaviour in sport	
Part 3 Additional Conditions relating to Criminal Convictions	
Consent	
Processing by not-for-profit bodies	
Personal data in the public domain	
Legal claims	
Judicial acts	
Administration of accounts used in commission of indecency offences involving children	
Extension of conditions in Part 2 of this Schedule referring to substantial public interest	
Extension of insurance conditions	

3. Ensuring Compliance with the Principles

There is no requirement to reproduce information which is recorded elsewhere – questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.

Accountability Principle

Question	Y/N	Details
Do we maintain appropriate documentation of our processing activities?	Y	DPIA; APD; Audit trails; Occurrence log updates; policy documents
Do we have appropriate data protection policies	Y	Overarching DP Policy
Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?	Y	See DPIA ref: AR0120

Principle (a) Lawfulness, fairness and transparency

Question	Y/N	Details
Have we identified an appropriate lawful basis for processing and a further	Y	UKGDPR Article 9.2(g) processing is necessary for reasons of substantial public interest, on the

Schedule 1 condition for processing special category/criminal offence data?		basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. UKGDPR Article 10 Schedule 1 Part 2, para 6 Statutory and government purposes
Do we make appropriate privacy information available with respect to the special category/criminal offence data?	Y	Yes - information is published on the SWP/GWP websites This is in addition to the general privacy policy.
Are we open and honest when we collect the special category/criminal offence data and do we ensure we do not deceive or mislead people about its use	Y	Yes – see above. Investigators and RFR Operators are also subject to the Code of Ethics

Principle (b): purpose limitation

Question	Y/N	Details
Have we clearly identified our purpose(s) for processing the special category/criminal offence data?	Y	See DPIA AR0120
Have we included appropriate details of these purposes in our privacy information for individuals?	Y	Yes
If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?	Y	Information is not used for a different purpose.

Principle (d): accuracy

Question	Y/N	Details
Do we have appropriate processes in place to check the accuracy of the special category/criminal offence data we collect, and do we record the source of that data?	Y	Yes – ongoing assessment of the FRT takes place to ensure that the Public Sector Equality Duty is met. The capture and processing of the data is auditable in police systems.
Do we have a process in place to identify when we need to keep the special category/criminal offence data updated to properly fulfil our purpose, and do we update it as necessary?	Y	Yes – this is documented in DPIA AR0120 – the subject image and biometric templates are not retained.
Do we have a policy or set of procedures which outline how we keep records of	Y	Yes the overarching privacy policy deals with individual rights and there is also a joint

mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?		information management policy. The Digital Service Division manages data quality and the Niche RMS allows officers to include updates and correction.

Principle (e): storage limitation

Question	Y/N	Details
Do we carefully consider how long we keep the special category/criminal offence data and can we justify this amount of time?	Y	No biometric data is retained; other information retained for audit purposes are kept under current management of police information retention periods **Retention and Erasure** <u>Particular to the FRT System</u> - Image of the Subject ('Probe Image') - MOPI retention of personal information - Biometric Template of Probe Image - immediately deleted in the FRT system. - Image Reference Database Candidate Images and Biometric Template (held on FRT System) – mirror MOPI retention periods for NICHE RMS <u>Source System – Niche Record Management System</u> 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

Do we regularly review our information and erase or anonymise this special category/criminal offence data when we no longer need it?	Y	As above
Have we clearly identified any special category/criminal offence data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?	N	No.

Principle (f): integrity and confidentiality (security)

Question	Y/N	Details
Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?	Y	A DPIA/Info Sec assessment has been carried out
Do we have an information security policy (or equivalent) regarding this special category/criminal offence data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?	Y	There is a separate information security policy
Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?	Y	Personal data processed by RFR is processed within the SWP 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 policies are applied 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. SWP 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 is also subject to a robust DPIA that is reviewed annually. All staff receive basic data protection training must undertake annual mandatory training for managing information. RFR Operators and those involved in the day to day maintenance of the RFR system receive training specific to data protection and FRT. Role based access is applied for RFR capabilities and only those in specialist teams who will use RFR regularly to maintain competence and understanding of use principles are provided access to utilise the RFR system. Access to the system is only provided on the completion of training and can be suspended remotely with immediate effect should concerns be raised in regard to use by an RFR Operator The systems used to process personal data allow SWP/ GWP to respond to individual rights requests and to erase or update personal data at any point in time where appropriate and where personally identifiable information regarding data subjects 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.

Review of APD

Review Date	Reviewer	Version	Actions	Date of next review
09/12/2020	S. Lloyd	0.1	Original Draft	31/12/2020
31/12/2020	S. Lloyd	0.2	DSD SMT Review	31/12/2021
12/01/2021	S. Lloyd	0.3	DPO Review	12/01/2021
14/04/2021	S. Lloyd	1	FRT Board Review	14/04/2022
29/09/2022	S. Lloyd	2	Review	29/09/2023
29/09/2023	B. Gwyer	3	Review – no changes	29/09/2024
09/10/2025	B. Gwyer	APD003a.i.	Update to new document	

			template and amendments	