



Data Protection Legislation

Appropriate Policy Document (APD)

Appropriate Policy Document for sensitive data processing within the Facial Recognition Technology (FRT) Equitability Study

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

Terms & Definitions: Unless otherwise defined in this FRT Policy, capitalised terms shall have the meaning given to them (in priority order) in the FRT Equitability DPIA Annex and the FRT Equitability Study Plan

August 2022

Version 1.2

Version Control

Version	Date	Author	Purpose
V1.0	01/07/2022	S. Lloyd	Original Draft
V1.1	03/08/2022	S. Lloyd	DPO review
V1.2	09/08/2022	S. Lloyd	SRO Review

Purpose

Policy to outline the SWP's governance and compliance against Section 42 Data Protection Act 2018

This is an APD annex (the **Annex**) to SWP FRT APD's. This Annex addresses the further data processing and privacy considerations relevant to protecting the rights and freedoms of data subjects in relation to the Equitability Study as further identified in the FRT Trial Plan Documents. It is further supported by the SWP LFR Application and LFR Written Authority Document, which is used to apply for, authorise and review an LFR Deployment.

Introduction

This policy document has been produced in accordance with South Wales Police' obligations under Part 3 of the Data Protection Act 2018 (DPA). It should be read alongside the South Wales 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 [Privacy Notice](#). Data protection policy specific to LFR is also to be found in the LFR Policy and Data Protection Impact Assessment (DPIA) and the Part 2 DPA 2018 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 and the wider FRT Equitability Study Documents together demonstrate that SWP's processing of sensitive data in respect of facial recognition technology is compliant with the requirements with Part 3, Section 42 of the DPA 2018. In compliance with Section 42(2) of the DPA 2018 it explains the procedures and measures for securing compliance with the LE data protection principles and explains the policies as regards retention and erasure of personal data.

This document should be treated as being complimentary to SWP general record of processing under S61 DPA 2018. It also complements SWP's policy on protecting special category and criminal convictions policy.

Equitability Study Objectives

Objective	Why the objective is necessary in terms of intrusion and strictly necessary in terms of data processing activity
A FR algorithms currently used/intended for use in policing	
To evaluate the performance of facial recognition technologies in an operational setting in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics	The FRT Equitability Study Plan (Section 1) and this Policy explains why it is critical to understand accuracy and equitability. The evaluation results will enable the UK Law Enforcement Community to: <ul style="list-style-type: none">• based on understanding how the algorithm performs decide with greater assurance whether and how best to configure FR technology for effective deployment on operational use cases;• ensure unnecessary data processing, minimising collateral intrusion and ensuring a proportionate approach – for example, including the use of other policing tactics, technologies or algorithms which exhibit a performance profile more honed to a particular use case;• continue to discharge its PSED obligations by continuing to take all reasonable steps to

Objective	Why the objective is necessary in terms of intrusion and strictly necessary in terms of data processing activity
	understand the algorithms especially when this study enables testing to be undertaken in the operational environment.
For each Operational Use Case:	
<p>(a) What is the accuracy of the facial recognition algorithms?</p> <ul style="list-style-type: none"> • LFR accuracy: True Recognition Rate and False Alert Rate as a function of the alert threshold • RFR/OIFR accuracy: True Recognition Rate as a function of the number of top matches returned 	<p>Assures policing on:</p> <ul style="list-style-type: none"> • the accuracy of the FRT algorithms – this supports making (i) necessity decisions (i.e. would the algorithm technically enable the legitimate aim to be achieved) and (ii) a proportionality decision (i.e. managing collateral in the context of algorithm performance), and • provides information on selection of thresholds and other parameters to attune algorithm performance to the operational requirement.
(b) What is the variation in accuracy between the demographic groups?	<p>Identifies the extent of any “demographic bias” when using an algorithm for a realistic FR operational use case. This allows the policing utility, legitimacy and risks of the algorithm to be considered, where possible mitigated, and any decision on use to be made on an informed basis.</p>
(c) Are the variations in accuracy large enough to be “statistically significant”	
(d) Are demographic performance variations similar over the three Operational Use Cases (RFR, LFR and OIFR)?	<p>Enables policing to assess potential differences between LFR/OIFR/RFR which may impact on operational deployment of use cases. This is relevant to algorithm selection and the operational design of FR systems to meet policing use cases. The understanding here will best enable police to meet their law enforcement purposes.</p>
(e) Are variations in accuracy affected by environmental factors (e.g. weather, illumination level, crowd density).	<p>Provides information of environmental factors that could increase/reduce accuracy and bias. This will allow policing to better plan for and use FR technologies – to maximise their effectiveness when used and in so doing, best achieve their law enforcement purposes.</p>
(f) How is the variation in accuracy affected by system factors (e.g.,	<p>Informs on effects of choice of Threshold / Watchlist composition on accuracy and bias. This helps minimise collateral intrusion and allows any</p>

Objective	Why the objective is necessary in terms of intrusion and strictly necessary in terms of data processing activity
algorithmic thresholds, composition of Watchlist/reference database)?	impact the composition of Watchlist/reference libraries may have on the performance of a FR system.
(g) Enable an appreciation of image quality on the performance of algorithms in order to better assess the utility of a FR system to generate a match.	Law enforcement rarely benefits from having 'perfect' images – even in more controlled environments such as custody. Image quality can vary depending on capture device, environmental conditions, means of sharing, compliance of the subject and many other factors. Yet, when submitted to the FR system, understanding the prospects of success (if there is a location/match to be made) is an important factor in making the necessity decision to process the data. This objective will be important to further knowledge in the area – especially when a FR system flags image quality as a consideration on ingestion of an image.
B Building capability to evaluate future Policing FR algorithms using representative data	
To collect a ground-truth dataset the UK Law Enforcement Community can use for future testing of other FR algorithms using a testing programme based on the retrospective analysis undertaken by the Equitability Study.	At present the UK Law Enforcement Community lacks operationally realistic datasets to bridge between NIST Tests and the operational environment. The Equitability Study addresses allows law enforcement to take the 'reasonable step' now, but the need will continue unless addressed for SWP and other forces going forwards. Examples include when a new algorithm is issued by a vendor, a use case changes or a further use case arises. Indeed many other forces will be unable to address this issue, as they lack the level of operationally realistic filler data holdings required in order to achieve a statistically significant equivalent to the Equitability Study as has been advised as being required by the National Physical Laboratory.

Objective	Why the objective is necessary in terms of intrusion and strictly necessary in terms of data processing activity
	<p>Therefore, a critical objective of the Equitability Study is to gather a curated operationally realistic dataset (volunteer), not only to achieve the above objectives but to fill this vital capability gap for the UK Law Enforcement Community for the future to allow repeats of the retrospective analysis undertaken by the Equitability Study to be undertaken to assess the performance of FR algorithms in the future.</p> <p>Retention of the volunteer data and footage (as further outlined in the DPIA Annex), with a three year review period will:</p> <ul style="list-style-type: none"> • Reduce/avoid the need to collect further personal data to run similar evaluations, but enable use of operationally realistic data for 'bench testing' going forward. This will increase the assurance available to SWP and the wider UK Law Enforcement Community (subject to agreeing licence terms) prior to their use of FR technology operationally. • Provide a means by which other UK law enforcement bodies can undertake an equivalent evaluation of their FR algorithms against their use case. For many forces, without the study and data, this would be an impossibility due to lack of resource, scientific expertise and a lack of the operational data needed to achieve a statistically significant study. This informs SWP 'strictly necessary' decision in relation to data processing • Allow 'side by side' comparisons between algorithms – especially over time when a new algorithm version is released. It avoids the need to reprocess the same data many times but instead compare back to existing findings and inform decisions as to when algorithms should be upgraded and the likely benefits that can be expected. • Will allow more informed procurement decisions. This is relevant not just to ensure the algorithm is high performing, but that it is so against the specific operational use case. It makes it possible to provide this 'real world'

Objective	Why the objective is necessary in terms of intrusion and strictly necessary in terms of data processing activity
	<p>performance assurance against operational use cases as part of procurement programmes rather than following them.</p> <p>Note - For the avoidance of doubt, the curated dataset to enable future testing will not be provided to FR vendors to train FR algorithms – this risks being self-defeating should algorithms be specifically trained to the test data whereby performance may not be replicated in wider operational conditions.</p>

DESCRIPTION OF DATA PROCESSED, INDIVIDUALS IMPACTED, PURPOSES AND SCOPE OF PROCESSING AND RETENTION PERIODS

Ser.	Personal Data Captured	Volunteer data subject(s) (y/n)	Collateral/public passing the camera data subject(s) (y/n)	Why the Personal Data is processed (use Key, maybe multiple entries)	How long is the Personal Data retained for in relation to Objective A.	How long is the Personal Data retained for in relation to Objective B.	Where the personal data is to be held following collection
1.	Name	Y	N	All	Retained until the Equitability Study Report is issued.	3 years review period	Metropolitan Police Service (MPS) Data Office (and DPO) for the purposes of separating the name and URN.
2.	Unique Reference Number	Y	N	All			MPS Data Office MPS TRI NPL (Objective A only)
3.	Contact Details and associated details on the Consent Form	Y	N	All			MPS Data Office
4.	Date of Birth (minimised to year of birth/age for Objective B)	Y	N	Study, Data			MPS TRI NPL (Objective A only)
5.	Self-defined gender	Y	N	Study, Data			
6.	Self-defined height	Y	N	Study, Data			
7.	Image(s) of volunteer	Y	N	Study, Data			
8.	Video of volunteer	Y	N	Study, Data			
9.	Image frames / video footage of all people passing through the Zone of Recognition	Y	Y	Study, Data			
10.	Perceived gender	Y	Y	Study, Data	Retained until the Equitability Study Report is issued.	3 years review period	MPS TRI NPL (Objective A only)
11.	Perceived age	Y	Y	Study, Data			
12.	Perceived height	Y	Y	Study, Data			
13.	Metadata (including location, date and time image/footage was taken)	Y	Y	Study, Data			
14.	Self-defined ethnicity and skin tone	Y	N	Study, Data	Retained until the Equitability Study Report is issued.	3 years review period	MPS TRI NPL (Objective A only)

Ser.	Personal Data Captured	Volunteer data subject(s) (y/n)	Collateral/public passing the camera data subject(s) (y/n)	Why the Personal Data is processed (use Key, maybe multiple entries)	How long is the Personal Data retained for in relation to Objective A.	How long is the Personal Data retained for in relation to Objective B.	Where the personal data is to be held following collection
15.	Biometric facial template	Y	Y	Study	See 'Template Retention Period' below.	Not part of Objective B. ¹	MPS TRI NPL (Objective A only)
16.	Perceived ethnicity and skin tone	Y	Y	Study, Data	Retained until the Equitability Study Report is issued.	3 years review period	
17.	Examples include perceived religious or philosophical beliefs (e.g. based on the clothing of the person passing), perceived data concerning health and perceived sexual orientation.	Y	Y	Study, Data	The footage/imagery from which the data may be perceived will be retained until the Equitability Study Report is issued.	The footage/imagery from which the data may be perceived will be subject to a 3 year review period.	MPS TRI NPL (Objective A only)
Study	In accordance with Section 35(2)(b) in relation to processing of personal data In accordance with Section 35(5) and Schedule 8, Paragraph 9 (b) and (c) in relation to sensitive processing.						
Data	In accordance with Section 35(2)(b) in relation to processing of personal data In accordance with Section 35(5) and Schedule 8, Paragraph 9 (b) and (c) in relation to sensitive processing.						
Indiv	In accordance with Section 35(2)(b) in relation to processing of personal data and Chapter 3 of the DPA 2018.						
All							

Retention periods where there is a variance from SWP LFR DPIA's	
Retention period	Rationale
Retained until the Equitability Study Report is issued.	This period of retention is necessary in order to achieve the objectives as part of the Equitability Study. Once the report has been validated, finalised and issues, the necessity to retain data for this purpose will have ceased.
Template Retention Period <ul style="list-style-type: none"> During an LFR deployment biometric facial templates are immediately and automatically deleted if no Alert is generated. If an Alert is generated the template is deleted as soon as possible and in any event within 24 hours (subject to retention for operational purposes in line with SWP's LFR DPIA). For retrospective analysis, templates can be generated from the footage/imagery. Templates generated as 	The LFR time periods align with SWP LFR DPIA's, weeding data where there is no need to retain it. The 24 hour period aligns with the SWP LFR DPIA and was selected there to allow time for a post-Deployment review. That review process may provide insight of value to the Equitability Study too in the context of the Alert generated and therefore has been reflected. In relation to the retrospective analysis, this reflects the duration which is necessary in order to achieve the trial objectives as part of the Equitability Study. It also reflects a deletion process prior to this long-stop data wherever possible. Once the report has been validated, finalised and issues, the necessity to retain data for this purpose will have ceased.

¹ Note – it is not necessary to retain biometric templates of those within the curated dataset. The templates are algorithm and vendor specific and therefore these would be generated by a future FR algorithm under study at the time (subject to a DPIA for that purpose).

<p>probes for searches will be deleted at the conclusion of each Test. All other biometric data (i.e. the research watchlist against which probes are searched and as specified in the FRT Equitability Study Plan) will be deleted no later than when the Equitability Report is issued.</p>	
<p>3 years review period</p>	<p>At present the UK Law Enforcement Community lacks operationally realistic datasets to bridge between NIST Tests and the operational environment – some public sector datasets are around a decade old and therefore do not provide sufficient operational realism. Much of law enforcement lacks the ability to undertake scientific research of the nature outlined by this Equitability Study yet have operational use cases which could be achieved through the use of FR. The Equitability Study requires developed technical knowledge, legal expertise, and data protection know how – combined with an operational use case and expertise. These skills are in short supply with few forces having access to all the practitioners needed. It also requires data holdings to use for research purposes. In line with a wider industry issue, many forces would not have the data holdings needed of the type, quality and realism needed to undertake the Equitability Study.</p> <p>A critical objective of the Equitability Study is to gather a curated operationally realistic dataset (footage and volunteer), not only to achieve the above objectives but to fill this vital capability gap for the UK Law Enforcement Community for the future. The three year period for review has been determined as a necessary and proportionate period for review on the following basis and will only result in the retention of data where the necessity case continues to be made out for it:</p> <ul style="list-style-type: none"> • Algorithms of relevance to law enforcement use cases are typically released on an 18/24 month cycle. The three year review period allows for a side-by-side comparison between algorithms to compare performance between products (in the context of continuing to minimise any undue impact from the use of the algorithm as part of the proportionality). This minimises repeated data collection and maximises the effective use of the data captured. • Image quality can vary and typically improves over time in terms of camera performance and the ability to mitigate the impact of environmental impacts. • Capital replacement cycles are typically based on a three year cycle – this may see the quality of images and the operational realism and value of the dataset to increase assurance beyond NIST tests potentially reduce beyond the three year period. This three year period provides a well-timed review period as a result as well as reflecting a period where capital spend cycles will inform procurement decisions

KEY POINTS REGARDING THE EQUITABILITY STUDY

Who has direction and control of the trial?

The trial is under the overall direction and control of the MPS Commissioner. Lindsey Chiswick (Director of Intelligence) is the senior responsible officer for the Equitability Study for the MPS. ACC Mark Travis is the senior responsible officer for the Equitability Study for SWP.

Who is the data controller for the trial?

The Chief Constable of SWP will be the data controller for the SWP LFR Operational Deployment and associated volunteer data capture (under their own DPIA and associated documentation) prior to undertaking a controller-to-controller transfer to the MPS.

Third parties involved to deliver the trial and their results (e.g. data processors / joint controllers)

- **Processor:** The NPL will be a processor to each of SWP and the MPS in a several capacity (i.e. SWP-NPL and MPS-NPL) appointed by way of data processing agreements.
- **Sharing/Controller – to controller transfer with licence:** The dataset retained, subject to the three year review period, will be made available to the UK Law Enforcement Community via a licence agreement to ensure the safeguards in the DPIA remain implemented by wider law enforcement. Other law enforcement bodies face the same issues as SWP with the need for operationally realistic data.
- **Note** - The algorithm / FR vendors (for any purposes relating to technical support) will not have access to the FR system when it is processing personal data and therefore are not processors for the purposes of the Equitability Study.
- **Note** - For the avoidance of doubt, the curated dataset to enable future testing will not be provided to FR vendors to train FR algorithms – this risks being self-defeating should algorithms be specifically trained to the test data whereby performance may not be replicated in wider operational conditions.

PART OF THE DPA 2018 UNDER WHICH THE PROCESSING WILL OCCUR

The Equitability Study will process personal data under Part III DPA 2018. Law Enforcement Purposes include the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Through achieving the Equitability Study objectives, SWP and law enforcement will be better able to understand its FR capabilities to make more refined necessity and proportionality decisions in pursuit of its legitimate law enforcement aims. Where sensitive processing is required, this will be necessary on the basis of Paragraph 9(b) and (c) of Schedule 8 – for scientific research and statistical purposes. The DPIA Annex outlines the rationale for Part III processing and applicable Schedule 8 grounds further as should be read as being included in this document.

DATA STORAGE

SWP has adopted risk mitigation points including the following in policy to ensure data security in relation to the storage of personal data:

- a) **Password security:** NPL will be following the password guidance policy set by the National Cyber Security Centre on all hardware and software used for the processing of STAR data. This includes advice and guidance for system owners responsible for determining password policies and identity management within their organisations. This guidance will be applied to the security of the standalone hardware with the NEC FR software installed.
- b) **Role access:** NPL access to the Equitability Study data will be limited to Dr Tony Mansfield and his assistant.
- c) **System Security:** The system, and algorithms have been assessed for meeting security standards and risk of compromise, and is air gapped from other networks. Data (such as imagery) will be transferred into the FR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine and wiped securely deleted at the conclusion of activity.
- d) **Physical Security:** The system itself is secured in a locked room, with key access through a central security office with full audit history.

THE RIGHT TO REQUEST DATA ERASURE

The right to erasure allows data subject to request erasure of their personal information. This enables data subjects to ask SWP to delete or remove personal information where there is no lawful reason for SWP to continue to process it. This right is not specific to the Equitability Study or FR more generally but applicable to all personal data processed by SWP. To facilitate individual rights further, the following considerations apply (in addition to those already in place via SWP LFR Policy Documents):

- a) **Volunteer Information:** All volunteers will be provided with detailed information about the Equitability Study, how their data is used and how they may exercise their individual rights and/or contact SWP for further details.
- b) **Approach to Volunteers to uphold individual rights:** Where volunteers have received payment to recompense subjects for their participation, the exercise of individual rights will not result in the claw-back of any payment – this reflects the genuine choice volunteers have to participate and agree to their processing of data.
- c) **The URN system:** Volunteers will be issued with a URN. The ability to reconcile a name to a URN will rest with MPS TRI under the stewardship of the MPS DPO and this is there to enable individual rights rather than any operational activity.
- d) **Awareness measures:** These are outlined below - they are extensive, reflect a transparent and open approach and equally apply here to ensure that individuals are aware that data is being processed for the purpose of the Equitability Study such that they may consider seeking to access it. The public passing the LFR system will benefit from prior awareness measures which link to SWP website and privacy information.
- e) **Systems used:** The FR systems used are capable of responding to updated data requests/deletion requests should a request be made to do so.
- f) **Designed in deletion:** During an LFR deployment biometric facial templates are immediately and automatically deleted if no Alert is generated. This

minimises the need to erase data by deleting data where there is no ongoing purpose for retention.

- g) **SWP Privacy Notice:** This provides that requests for data erasure or restriction may be provided to the Data Protection Officer/Information Security Officer at: Dataprotection@south-wales.police.uk.
- h) **SWP website:** This provides the public with a copy of the SWP Privacy Notice that details how the right to erasure or restriction may be exercised.
- i) **SWP LFR Documents / FRT Equitability Study Trial Documents:** These provide detailed safeguards around the use of data and how it will be held and managed. This is further supported by the processing agreement with NPL to ensure individual rights requests can be facilitated.
- j) **SWP policy:** and guidance is provided by the SWP's Data Protection Officer/Information Security Officer to ensure SWP complies with this legal obligation.
- k) **The DPO Role:** SWP DPO is an integral role to the processing of personal data and the upholding of individual rights, providing scrutiny, challenge, advice to do so.

THE ACCOUNTABILITY PRINCIPLES

SWP has in place appropriate technical and organisational measures to meet the requirements of the accountability principle. These include:

- data protection policies and other documentation which in the context of FR include the FRT Equitability Study Documents, SWP Privacy Notice, and SWP's policies on protecting special category and criminal convictions policy;
- detailed security measures relating to the FR system;
- a 'data protection by design and default' approach to the FR system;
- data protection measures and policies to record and, where necessary, report personal data breaches;
- the appointment of a data protection officer;
- responding to guidance and documentation produced by the Surveillance Camera Commissioner, the Biometrics Commissioner and the Information Commissioner; *and*
- a process for ongoing review with the Data Protection Officer (DPO) also having oversight of this via the SWP Facial Recognition Technology Board.

PRINCIPLE 1: LAWFULNESS

The legal context to support the need for the Equitability Study: There are a number of legal obligations which cause it to be necessary to understand the performance of FR algorithms in the context of overall accuracy and demographic differential performance. These include (with further legal detail being outlined in the DPIA Annex):

- a) **Human Rights Act 1998:** The use of FR technology typically engages human rights considerations where interference with qualified rights needs to be justified on the basis of necessity to achieve the legitimate aim. It therefore follows that the technical ability to achieve the legitimate aim needs to be considered and understood. It also follows, as part of the proportionality

analysis that the degree to which those not of interest to the police are subject to interference is relevant.

- b) For example, those added to a LFR Watchlist or passing a LFR system have their Article 8 rights engaged as a result of the biometric data processing activity. Similarly for OIFR and RFR, those submitted as a probe image for searching result in biometric data processing. Amongst other requirements, as a qualified right, the interference can be justified where it is necessary and proportionate to the legitimate aim sought.
- c) For LFR: if locating someone is necessary, this raises the question 'necessary for what'. The 'what' – or in legal terms, the legitimate aim, means there needs to be an understanding as to the prospects of an Alert being triggered if the person sought passes through the Zone of Recognition. Why use LFR if it is unlikely at a technical level to generate the Alert? Similarly, if it was known that an algorithm would generate a high number of false alerts, this consideration should be factored into the proportionality consideration (and mitigated where it is possible to do so).
- d) For RFR and OIFR: if it becomes necessary to submit a probe image for searching against an image reference library to progress an investigation, it follows that if a corresponding image of the subject is in the library, there needs to be an understanding as to the likelihood of that being returned as a potential match. Otherwise the probe image may lack a point or otherwise provide false confidence a subject is not known to the police if a potential match is not returned.
- e) If it was known a particular algorithm was particularly weak at locating/matching a person of a particular demographic, the necessity for use of that particular FR algorithm may not be made out – other tactics (potentially including more intrusive ones) with stronger prospects of success should then be considered as part of the necessity and proportionality decision as to how to achieve the legitimate aim.
- f) Further, this will be relevant not just when using the algorithm, but procuring FRT algorithms too. The algorithm's performance needs to respond to SWP's particular use case for the FR technology.
- g) Some use cases will require uniform level of performance across a broad range of demographics – e.g. RFR for investigations, any algorithm will need a high level of accuracy and *uniform* performance across demographics – reflecting the community SWP serves.
- h) It is also conceivable, as technology continues to develop that FR algorithms may also be used for very specific use cases. In those circumstances, the focus on accuracy and demographic performance needs to be made in the context of performance against that specific use case in order to maximise the chances of achieving the legitimate aim and minimising the impact on those who will actually be subject to the processing.
- i) Importantly, the Equitability Study will provide the UK Law Enforcement Community with a much needed means by which to assess algorithms using operationally realistic data to ensure they can better select, anticipate the performance characteristics of, and mitigate adverse impacts arising from and use of algorithms. This will enable the police to better deliver on their law enforcement purposes in a proportionate way; and for SWP, to be the best at understanding and responding to the needs of all our communities.

- j) **Data Protection Act 2018:** Section 35(5) of the DPA 2018 requires that biometric data processing in relation to FR algorithms needs to be to a strict necessity standard for a law enforcement purpose.
- k) For similar reasons to those explained in the context of human rights, a technical understanding as to the prospects of the algorithm being able to help SWP achieve that purpose is needed in order to make a necessity and proportionality decision to process data or not.
- l) Furthermore – compliance with the data protection principles underpin the driver to conduct an operational Equitability Study, particularly in two respects:
- a) Principle 1 - the processing of personal data for any of the law enforcement purposes must be fair. Fairness in this context includes how the algorithm performs to ensure there is an equality of impact and effectiveness and any adverse impact can be mitigated, and residual effect, justified. To this end it is important to understand how the algorithm performs.
- b) Principle 4 – this principle concerns data accuracy, and in the context of the algorithm, the statistical accuracy of the algorithm. Again, understanding algorithm performance is important in order to be able to assess any risks to data subjects and seek to mitigate them. For example, this:
- may result in more focused training to those who undertake human-in-the-loop reviews;
 - may see details of algorithm performance shared with any RFR potential matches to another police force investigating a crime so they are fully informed and understand how the match was generated. This could then inform that police force's use of the details for their investigation and avoid a risk to the data subject which may come from over-reliance on the data or a failure to fully understand what might be needed from the human-in-the-loop.
- m) **Equality Act 2010:** The terms of the Public Sector Equality Duty (PSED) are set out in section 149(1) of the Equality Act 2010 as follows:
- A public authority must, in the exercise of its functions, have due regard to the need to—*
1. *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*
 2. *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*
 3. *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.”*
- n) Whilst the courts have made clear that the ‘impossible’ is not required, there is a need to take reasonable steps for a police force to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias. The ‘reasonable steps’ obligation is therefore one which needs to be set in the context as to what is reasonable and possible in the context of the FR algorithm and how it will be used. SWP has taken reasonable steps to be informed prior to use for FR technology given its evaluation of the NIST Tests (see below) and an absence of further, more relevant data. Such data necessitates testing in an operational environment – reflective of real-life data and the operational need. The Equitability Study

therefore reflects that SWP will continue to take ‘reasonable steps’ and is reflective of the going nature of the PSED.

o) **Caselaw:** The ‘*Bridges*’ Court of Appeal judgment² considered SWP’s use of FR technology in the live context at specific deployments. Whilst the findings are relevant to that case, they have wider application to the lawful use of LFR, wider LFR use-cases and other FR technology applications within law enforcement. Key points relevant to the Equitability Study include:

- **Legal basis:** The Court of Appeal recognised the sufficiency of the legal basis for FR (including the common law and S.64A PACE).

“The short answer, in our view, to this submission is that the legal framework which regulates the deployment of AFR Locate [SWP’s name at the time for LFR] does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined.”

- **The PSED, where the focus should be and the ‘Reasonable Steps’ test:** The Court of Appeal recognised, applying the ‘reasonable steps’ test, that the need to make enquiries as to the performance of the algorithm, focusing particularly on race and sex – conditioned on what is reasonable in the context (emphasis added):

“We acknowledge that what is required by the PSED is dependent on the context and does not require the impossible. It requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex.”

“all police forces that intend to use [LFR] in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.”

PRINCIPLE 1: FAIRNESS:

Accessibility and Foreseeability: The Equitability Study benefits from (i) published statutory legislation and (ii) a Court of Appeal judgement from the Bridges case. Additionally to support accessibility and foreseeability SWP has published its legal mandate for LFR and will publish the DPIA Annex and this document which sets out the legal position that supports the Equitability Study. To increase accessibility and to ensure the public can read and understand that legal framework in a way which is applied to the Equitability Study so they can foresee how it may be relevant to them:

- a) SWP FR Webpages will include the DPIA Annex, this document and publish other FRT Equitability Study Trial Documents.

² <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>

- b) SWP LFR Deployments will include specific signage and leaflets which provides details on the additional data processing associated with the Equitability Study.
- c) The use of the NPL and the greater independence, scientific and technical rigour this brings to the study, in conjunction with the SWP Digital Services Division (DSD) support helps ensure the project is foreseeable and officer discretion limited. This approach isolates the technical analysis and research data processing from mainstream policing, ensures a trial plan has been produced and will be followed with scientific rigour.
- d) To ensure consistency in how the dataset is managed by law enforcement for future analysis a licence mirroring the standards reflected in the DPIA Annex for SWP use will be a pre-condition to any sharing.

Making available appropriate privacy information: SWP has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of SWP to be open and transparent (wherever appropriate and possible) about how data is processed. A key measure is the publication of SWP Privacy Notice, SWP policies on protecting special category and criminal convictions, and key documents relating to the Equitability Study on the SWP website. Whilst SWP is not required to publish a number of these documents, it has elected to do so. Further points in relation to making available information follow:

- a) **Volunteer Information:** All volunteers will be provided with detailed information about the Equitability Study and how their data is used.
- b) **Signage and social media for those passing the FR system:** The overt nature of the LFR Deployments is already highlighted through social media and the use of signage on the day, which will be prominently placed on the approach to the LFR cameras, outside the Zone of Recognition. The social media and signage for deployments where the Equitability Study is overlaid will flag this further purpose and link to SWP website where further documents and information is published.
- c) **Publication:** Whilst SWP is not required to publish a number of the Equitability Study documents, it has elected to do so in line with its commitment to transparency. This is to help an important measure to inform the public as to how SWP plans to undertake the Equitability Study, including the public passing an LFR system and those who may have their data processed as part of the retrospective analysis in order to understand the standards SWP, as a public body, operates to. In this way, SWP's use of FR for the Equitability Study is both foreseeable and assessable. The published documents provide information as set out in the table below:

Key documents available to the public	Information included
SWP Privacy Notice:	<ul style="list-style-type: none"> • Data Controller identity and contact details • Data Protection Officer details • The scope and purposes for processing personal data by the SWP • Data retention periods • Data sharing arrangements • Data security

	<ul style="list-style-type: none"> • Rights as a data subject (including access, rectification and erasure) • Complaints (including the right to make a complaint to the ICO and contact details).
SWP policy on protecting special category and criminal convictions	<ul style="list-style-type: none"> • SWP's approach in relation to protecting and processing special category and criminal convictions data in relation to the data protection principles • The responsibilities of the Data Controller • Information relating to erasure and retention • How further information may be sought.
Existing SWP LFR Documents – already published	
SWP LFR Legal Mandate	<ul style="list-style-type: none"> • The lawful basis for processing data in relation to LFR. Including in relation to: <ul style="list-style-type: none"> ○ Common law policing powers ○ Police and Criminal Evidence Act 1984 ○ Human Rights Act 1998 ○ Equality Act 2010 ○ Protection of Freedoms Act 2012 ○ Data Protection Act 2018 ○ Freedom of Information Act 2000
SWP Policy Document	<ul style="list-style-type: none"> • An outline, strategic intent and objectives for the use of LFR and how personal data will be used by the LFR system • Key terms used across SWP LFR Documents • Data retention periods applicable to LFR
SWP LFR Standard Operating Procedure Processes	<ul style="list-style-type: none"> • Outlines measures relevant to considering where LFR can be Deployed by the SWP. • Watchlist considerations including the basis on which images may be added to a Watchlist and considerations relevant to the sources of non-police originated imagery. • Provides that during any policing operation where LFR is Deployed officers will be available to assist member of the public with queries, and: <ul style="list-style-type: none"> ○ signs publicising the use of the technology must be prominently placed in advance (outside) of the Zone of Recognition; and ○ any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. • Both of these measures will be easy to read and together will ensure those passing the LFR system/who are Engaged by it will have the opportunity to seek further information. Both the signs and leaflets will typically provide an accessible QR code and website link to SWP website for more information.
SWP LFR DPIA	<ul style="list-style-type: none"> • Describes the nature, scope, context and purposes of the processing. • Assesses necessity, proportionality and compliance measures. • Identifies and assesses risk to individuals.

	<ul style="list-style-type: none"> Identifies any additional measures to mitigate those risks.
SWP FRT Appropriate Policy Documents	<ul style="list-style-type: none"> Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the DPA 2018. Explains how SWP complies with the Law Enforcement data protection principles. Outlines policies as regards the retention and erasures of personal data. Explains how the processing of special category data under Part 2 Data Protection Act 2018 and Article 9 General Data Protection Regulation
SWP LFR EIA	<ul style="list-style-type: none"> Explains SWP's approach to its responsibilities in relation to the Public Sector Equality Duty.
Further FRT Equitability Study Trial Documents – to be published	
FRT Equitability Study Plan	<ul style="list-style-type: none"> Describes the test objectives and necessity case for them. Outlines the testing methodology and the purposes of each stage of the test methodology. Outlines the process and strategy in relation to demographic testing, data subject numbers and breakdown, images and footage to be captured / processed and the rationale for the numbers and sources selected. Outlines the retrospective test strategy, tests to be undertaken and rationale for them. Explains the performance analytic metrics selected, the process for completion and the ongoing need for the retention of the curated dataset for future FR evaluation.
FRT Equitability Study DPIA Annex	<ul style="list-style-type: none"> Describes the nature, scope, context and purposes of the processing over and above the SWP LFR DPIA (and as visually shown in the FRT Equitability Study Process Summary). Assesses necessity, proportionality and compliance measures. Identifies and assesses risk to individuals. Identifies any additional measures to mitigate those risks.
FRT Equitability Study EIA Annex	<ul style="list-style-type: none"> Explains the SWP's approach to its responsibilities in relation to the Public Sector Equality Duty.
FRT Equitability Study Process Summary	<ul style="list-style-type: none"> Outlines the processing activities for the Equitability Study and places them in the context of an operational LFR Deployment. Outlines the documentation and relationship between SWP, MPS, and NPL in the context of controllership and processors and the associated documentation to support this.
FRT Equitability Study Appropriate Policy Annex	<ul style="list-style-type: none"> Explains how the processing of sensitive personal data for the purposes of the Equitability Study is compliant with the requirements of Part 3, section 42 of the DPA 2018. Explains how SWP complies with the Law Enforcement data protection principles. Outlines policies as regards the retention and erasures of personal data.

Fairness in relation to data processing: The Equitability Study falls within obligations on policing to understand the technology it uses and to ensure best

practice use when policing the community. To ensure fairness a number of mitigation and best practice points have been adopted:

- a) **Equitability Study Design:** The Equitability Study is governed by a FRT Equitability Study Plan which sets out up front the testing to be undertaken. This has been designed and informed by the NPL, a body with recognised expertise for testing in the area. This ensures a rigorous, justified, predictable and expert-led approach is adopted. As a result the data processing to be undertaken remains bounded to what is really needed and proportionate.
- b) **Adherence to ISO standards:** The evaluation will be conducted in accordance with international standards for testing and reporting the performance of biometric recognition systems: ISO/IEC 19795-1 and ISO/IEC 19795-2. In the terminology of the standards for biometric performance testing and reporting, the performance will be evaluated as a “technology evaluation”.
- c) **Awareness measures:** These are outlined above in relation to ‘legal risk’ - they are extensive, reflect a transparent and open approach and equally apply here to ensure that unexpected data processing is mitigated in so far as possible. The public passing the LFR system will benefit from prior awareness measures and are not obliged to pass the LFR system. The public also benefit from substantial published primary legislation and case-law in the area of relevance to the Equitability Study.
- d) **Fairness in relation to volunteer probe images:** Whilst the processing of data is strictly necessary, all volunteers will be provided with detailed information about the Equitability Study and how their data is used. Their agreement to participation, consistent with their volunteer status will be sought and they will have the ability to withdraw participation should they wish to do so.
- e) **Mitigating against unexpected processing:** To avoid the risk of ‘seepage’ into operational policing or adverse impact of using a person’s name – two mitigations apply which reflect a data protection by design approach. The use of the NPL and SWP DSD ensures the Equitability Study is separated from operational policing with the output purely focused on the objectives of the study. This is reinforced by the use of URNs as opposed to names. The ability to reconcile a name to a URN will rest with MPS TRI under the stewardship of the MPS DPO and this is there to enable individual rights rather than any operational activity.
- f) **Wider fairness when using the data set:** To mitigate the risk that wider law enforcement may not observe the same high standards as SWP seeks to adopt, those who make use of the data set will be required to enter into a binding licence to use the data set which will mirror the conditions in the DPIA Annex. Further FR analysis using the data set within the review period will also be subject to an approved DPIA to such testing.

Principle 2: Purpose limitation: The Equitability Study involves:

- a. New data being processed for a law enforcement research purpose: This is reflective of the volunteers’ participation, both in terms of providing probe images, and passing through the Zone of Recognition in order to create footage which may be subject to retrospective analysis for the purposes in line with the FRT Equitability Study Plan.

- b. Existing data being processed for a further, law enforcement research purpose: This is reflective of the public passing through the Zone of Recognition for the purposes of the Equitability Study in addition to SWP conducting an operational LFR Deployment.

Whilst the Equitability Study therefore reflects additional purposes for processing, in accordance with this Principle, there is also a need to ensure that processing in line with the FRT Equitability Study Plan remains specific, explicit and legitimate and is not subject to further, unauthorised or illegitimate purpose creep. To do this, the following points have been adopted:

- a. **Compatibility with original purpose**: In relation to the passing public, the Equitability Study is complimentary to the LFR deployment purposes – i.e. seeking to use LFR by preventing and detecting crime, bringing people to justice and ensuring public safety, whilst minimising and mitigating the impact on the passing public. Both purposes will apply at the same time to the passing public – there is no retrospective ‘purpose creep’. The Equitability Study is reflected in the SWP LFR DPIA as part of the action plan on fairness, is a planned next ‘reasonable step’ and ensures FR algorithms can be assessed in an operational context as to accuracy and bias. The additional awareness measures described in the DPIA Annex reinforce public understanding.
- b. Whilst this processing is undertaken in a Part III context, it is instructive that UK GDPR (Recital 50) says that compatible purposes to an original purpose include scientific research and statistical purposes and in a para 9, Schedule 8 DPA context, these are the grounds cited to justify the sensitive processing.
- c. **The FRT Equitability Study Plan**: The creation and use of this document brings professional and scientific rigour to the testing process. Its publication (and other awareness raising measures outlined in this document) ensures that SWP is clear and transparent from the outset what data will be captured or otherwise processed, how it will be processed and why it will be processed. It ensures the study is bounded and implements a ‘Data Protection by Design and Default’ approach.
- d. **Licence and future use**: The retention for the dataset for future FR analysis is limited in a number of ways (i) a need for a future approved DPIA (ii) an organisation limit – for UK law enforcement bodies, (iii) a legal limit – where the body is not SWP a licence agreement will be required to ensure legal obligations are imposed to mirror and uphold the safeguards in the DPIA.
- e. **Watchlists during an operational LFR Deployment**: During an operational Deployment, where volunteers are passing the LFR system, their images will be technically segregated from any operational Watchlist. Likewise, the operational Watchlist is not retained following the Deployment (per SWP LFR Documents) and therefore will not be subject to retrospective analysis with imagery from the Equitability Study. This implements a ‘Data Protection by Design and Default’ approach.
- f. **Research images**: The retrospective analysis will be undertaken using dedicated images (comprising volunteer) via the NPL and MPS TRI. This key ‘Data Protection by Design and Default’ point ensures segregation from operational policing and means there are no operational

consequences to those subject to retrospective analysis – its purpose being purely research in connection with the Equitability Study. The team and processing is located away from operational investigations and uses dedicated IT resource to reinforce this position.

- g. **Regular review and purpose limitation:** The Equitability Study will be subject to regular review to ensure it is in compliance with the FRT Equitability Study Plan and that remains necessary, proportionate and effective in achieving its objectives. Should any further processing purposes be identified, these will need to be articulated, authorised by the SRO in consultation with the DPO.

Principle 3: Data minimisation

The Equitability Study and DPIA Annex provides that SWP will only process data that is relevant and proportionate to its law enforcement policing purposes. There are a number of observations, systems and processes in place to ensure this. These are set out below:

- a. **Study design:** The NPL has been carefully selected as a data processor and advisor on the design of the study (adopting a data protection by design and default approach) – their expertise has helped design the Equitability Study.
 - Notably sections 5 and 6 of the FRT Equitability Study Plan sets out in detail the data subjects to be used in the study and why they are needed to achieve the objectives. There is a direct link between the objectives and all categories of data subject that fall within this this Equitability Study.
 - Section 5 also addressed the need for crowd subjects to pass the LFR system and why this needs to occur on an operational LFR deployment – therefore using members of the public – Section 5.5.3 on realism underpins this position and supports the judgment that the objectives could not be achieved by actors, or not involving the public. To mitigate the risk of processing more crowd data than needed, the study provides reference to monitoring the flow count of the passing public at Section 5.5.3.
 - In considering the impact and data risk to the crowd data subject, it is notable that ‘Bridges’ in that case recognised the intrusion as ‘negligible’. The court noted:
“An impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement.”
- b. **System design:** The FR systems to be evaluated undertake checks on ingestion to flag images of poor quality. The NPL will ensure that those which do not match the quality needed for use are therefore weeded out to avoid irrelevant data processing.
- c. **Regular review:** The Equitability Study will be subject to regular review to ensure it is in compliance with the FRT Equitability Study Plan and that remains necessary, proportionate and effective in achieving its objectives. Should it become apparent that irrelevant data processing is occurring, NPL will notify the Operational Lead for FR at SWP who has been empowered by the SRO to pause the Study.

Principle 4 Accurate and up to date

SWP is mindful of the potential damage and distress to data subjects, organisations, and to third parties if inaccurate data is processed in any way. To mitigate this, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing. There are a number of measures, observations and controls in place to ensure compliance with this principle:

a. In relation to inaccuracies in the data itself:

- The need for realism in the data used: The Equitability Study relies on the operational realism of the data to reach valid findings – this includes the data used. Therefore points such as Subject and Environmental Variables are necessary and important in order to assess any difference in performance between NIST Tests and operational conditions.
- Quality of Watchlist Images: When an image is ingested into the FR system, the system assesses image quality and suitability for matching, in order to allow SWP personnel to consider and manage the risk that poor quality images might generate False Alerts and therefore the realism and suitability to include it for the purposes of the Equitability Study.
- Distinguishing Data Subjects: During an operational Deployment, where volunteers are passing the LFR system, their images will be segregated from any operational Watchlist. Likewise, the operational Watchlist is not retained following the Deployment and therefore will not be subject to retrospective analysis of comingled with imagery from the Equitability Study. This implements a 'Data Protection by Design and Default' approach.
- NPL performance: NPL are responsible for the accuracy of volunteer data capture, the curated data set and the conduct of the test in accordance with the Equitability Study. NPL similarly have obligations to identify and flag to SWP incidences of inaccurate data processing where a data breach results. NPL performance is subject to audit and oversight by SWP – including Data Protection Officer/Information Security Officer, SWP DSD from data and technical perspectives.
- Individual rights: the ability to exercise individual rights is considered in this policy and the DPIA Annex.

b. In relation to algorithm performance:

- Prior due diligence: The ICO has provided helpful guidance on their expectations for statistical accuracy. They note that the accuracy principle “does not mean that [the LFR] system needs to be 100% statistically accurate to comply with the accuracy principle.” The ICO does however recognise the importance of considering the accuracy of the LFR system at the outset, including evaluating claims made by the vendor. In this respect SWP has paid close regard to the NIST findings. In relation to NIST, this paper notes:

“SWP’s facial recognition system uses an algorithm from a leading vendor, NEC. The NIST Test report published in 2018 evaluated over 200 algorithms for their accuracy. Its findings state that:

“NEC, which had produced broadly the most accurate algorithms in 2010, 2013, submitted algorithms that are substantially more accurate than their June 2018 versions and on many measures are now the most accurate”.”

“In March 2017, NIST also published a Face In Video Evaluation (FIVE) report. Unlike the other NIST Tests, the FIVE test involved the use of video footage as opposed to static images. This is of particular interest to the Met because this aligns more closely to the Met’s use of facial recognition in a ‘live’ - video context. The NEC algorithm was found to be the most accurate across the different measures with a True Positive Identification rate of 82% at a corresponding False Positive Identification Rate of 0.4%.”

- As a result of this detailed due diligence and further analysis by SWP DSD in relation to the NEC retrospective algorithm (which more closely aligns to the NIST tests still) SWP is content that the algorithms used are already ‘best of breed’ and capable of meeting operational use cases in the way in which they perform. This ‘Equitability Study’ is therefore only processing data using algorithms where prior due diligence indicates suitability/sufficient accuracy and that is then appropriate to test of any variations in performance when moving from NIST Tests to operationally realistic data. This approach will be reflected (as part of the ‘reasonable steps’ test to future algorithm selection and testing using the data gathered and retained from this project.
- Segregation from operational policing activity: To avoid the risk of any inaccuracy in the algorithm under review having law enforcement consequences to a data subject during the retrospective analysis phase – two mitigations apply which reflect a data protection by design approach. The use of the NPL and SWP DSD ensures the Equitability Study is separated from operational policing with the output purely focused on the objectives of the study. This is reinforced by the use of URNs as opposed to names. The ability to reconcile a name to a URN will rest with MPS TRI under the stewardship of the MPS DPO and this is there to enable individual rights rather than any operational activity.

Principle 5: Data is kept for no longer than necessary

The information will be retained in line with the FRT Equitability Study DPIA Annex. The retention periods selected have been selected based on the following summary rationale:

Retention periods where there is a variance from the SWP LFR DPIA	
Retention period	Rationale
Retained until the Equitability Study Report is issued.	This period of retention is necessary in order to achieve the objectives as part of the Equitability

	<p>Study. Once the report has been validated, finalised and issues, the necessity to retain data for this purpose will have ceased.</p>
<p>Template Retention Period</p> <ul style="list-style-type: none"> • During an LFR deployment biometric facial templates are immediately and automatically deleted if no Alert is generated. • If an Alert is generated the template is deleted as soon as possible and in any event within 24 hours (subject to retention for operational purposes in line with the SWP LFR DPIA). • For retrospective analysis, templates can be generated from the footage/imagery. Templates generated as probes for searches will be deleted at the conclusion of each Test (see section 8.7 of the Equitability Study). All other biometric data (i.e. the research watchlist against which probes are searched and as specified in the FRT Equitability Study Plan) will be deleted no later than when the Equitability Report is issued. 	<p>The LFR time periods align with the SWP LFR DPIA, weeding data where there is no need to retain it. The 24 hour period aligns with SWP LFR DPIA and was selected there to allow time for a post-Deployment review. That review process may provide insight of value to the Equitability Study too in the context of the Alert generated and therefore has been reflected.</p> <p>In relation to the retrospective analysis, this reflects the duration which is necessary in order to achieve the trial objectives as part of the Equitability Study. It also reflects a deletion process prior to this long-stop data wherever possible. Once the report has been validated, finalised and issues, the necessity to retain data for this purpose will have ceased.</p>
<p>3 years review period</p>	<p>At present the UK Law Enforcement Community lacks operationally realistic datasets to bridge between NIST Tests and the operational environment – some public sector datasets are around a decade old and therefore do not provide sufficient operational realism. Much of law enforcement lacks the ability to undertake scientific research of the nature outlined by this Equitability Study yet have operational use cases which could be achieved through the use of FR.</p>

The Equitability Study requires developed technical knowledge, legal expertise, and data protection know how – combined with an operational use case and expertise. These skills are in short supply with few forces having access to all the practitioners needed. It also requires data holdings to use for research purposes. In line with a wider industry issue, many forces would not have the data holdings needed of the type, quality and realism needed to undertake the Equitability Study.

A critical objective of the Equitability Study is to gather a curated operationally realistic dataset (footage and volunteer), not only to achieve the above objectives but to fill this vital capability gap for the UK Law Enforcement Community for the future. The three year period for review has been determined as a necessary and proportionate period for review on the following basis and will only result in the retention of data where the necessity case continues to be made out for it:

- Algorithms of relevance to law enforcement use cases are typically released on an 18/24 month cycle. The three year review period allows for a side-by-side comparison between algorithms to compare performance between products (in the context of continuing to minimise any undue impact from the use of the algorithm as part of the proportionality). This minimises repeated data collection and maximises the effective use of the data captured.
- Image quality can vary and typically improves over time in terms of camera performance and the ability to mitigate the impact of environmental impacts.
- Capital replacement cycles are typically based on a three year cycle – this may see the quality of images and the operational realism and value of the dataset to increase assurance beyond NIST tests potentially reduce beyond the three year period. This three year period provides a well-timed review period as a result as well as reflecting a period where capital spend cycles will inform procurement decisions

In addition to explicit retention periods set out by data type, the following further points also apply:

- a. **System design:** There are a number of points within the way the FR systems assessed work which uphold Principle 5:
 - Deletion of biometric data where an LFR system does not generate an Alert – this being consistent with the ‘Bridges’ decision and designed into the system,
 - For retrospective analysis biometric probe data will be deleted at the conclusion of each Test (see section 8.7 of the Equitability Study). All other biometric data (i.e. the research images against which probes are searched – and as specified by the FRT Equitability Study Plan) will be deleted no later than when the Equitability Report is issued. This process has been designed into how the systems are used and returned by NPL and reflected in the NPL Processing Agreement.
- b. **Licence and future use:** The retention for the dataset for future FR analysis is limited in a number of ways (i) a need for a future approved DPIA (ii) an organisation limit – for UK law enforcement bodies, (iii) a legal limit – where the body is not SWP a licence agreement will be required to ensure legal obligations are imposed to mirror and uphold the safeguards in this DPIA.
- c. Actions carried out within the FR systems are audited and logged in accordance with S.62 DPA.

Principle 6: Data security

The FR system includes a number of physical and technical security measures. These include:

- a. **Password security:** NPL will be following the password guidance policy set by the National Cyber Security Centre on all hardware and software used for the processing of STAR data. This includes advice and guidance for system owners responsible for determining password policies and identity management within their organisations. This guidance will be applied to the security of the standalone hardware with the NEC FR software installed.
- b. **Role access:** NPL access to the Equitability Study data will be limited to Dr Tony Mansfield and his assistant.
- c. **System Security:** The system, and algorithms have been assessed for meeting security standards and risk of compromise, and is air gapped from other networks. Data (such as imagery) will be transferred into the FR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine and securely deleted at the conclusion of activity.
- d. **Physical Security:** The system itself is secured in a locked room, with key access through a central security office with full audit history.

Policy document Sign-Off

Person completing the APD	Name (in capitals)	Scott Lloyd Chief Inspector
	Date:	01.07.2022
Data Protection Officer	Name:	Louise Voisey
	Date:	03.08.2022
Senior Responsible Officer	Name:	Chief Supt. Belcher
	Date:	09.08.2022