



STAFFORDSHIRE
POLICE

Data Protection Impact Assessment

RFR (retrospective facial recognition)

Stage 2

A Data Protection Impact Assessment (DPIA) is a mandatory requirement under the Data Protection Act (2018). Publication improves transparency and can increase the public's understanding of how their information is used.

The Stage 2 DPIA has been identified as required for this project.

In this stage of the DPIA process the Project manager or Information Asset owner must provide full details about the lifecycle of the data and the risks associated with the proposal. The information provided will supplement the information provided in Stage 1.

The aim of this process is to identify and mitigate risks.

Upon completing the Stage 2 DPIA template the Project Manager and Information Asset Owner (IAO) will review, sign off and send a copy to the Deputy Data Protection Officer (DDPO). The DDPO will then seek the views of the Information Security Officer (ISO). The DPIA will also be reviewed and signed off by the Data Protection Officer (DPO). If the DPO thinks that the risks are High, then the force Senior Information Risk Officer (SIRO) will be consulted. The SIRO may at this point ask that additional work is carried out or may decline the proposal and not accept any risks identified.

If the DPIA identifies a high risk(s) and measures cannot be undertaken to mitigate or reduce the risk then there is a requirement for the Force to consult with the Information Commissioner's Office (ICO). Consultation with the ICO will be undertaken by the Information Governance Team.

Should you have any queries in relation to the Data Protection Impact Assessment Process then please contact the Deputy Data Protection Officer at SPDPO@staffordshire.police.uk

OFFICIAL-SENSITIVE
(Update when complete)

Version	Version date	Requester of change	Summary of change(s)
V1.0	Oct 2024		First draft
V1.1	Nov 2024		additions
V1.2	Nov 2024		Additions to 7.2
V1.3	Nov 2024		questions answered
V1.4	Dec 2024		Added in MoPI risk
V1.5	Dec 2024		Additional questions answered 9.2 and 10.1 and risks from project risk log
V1.6	Dec 2024		Amended to include Phase 2. Amendments made to Section 6, 7.1, 7.2 , 8.1 and 9.4.
V1.7	Jan 2025		Risk added around data deletion in 10.1
V1.8	Jan 2025		

DOCUMENT REFERENCES

Ref	Document Name	Version Number

Sign-Off Authority Name	Role	Date	Signature
	Senior Information Asset Owner		
	Information Asset Owner		
	Project Manager		
Information Governance sign off		Low and Medium Risks	
	Deputy Data Protection Officer		

OFFICIAL-SENSITIVE
(Update when complete)

	Information Security Officer		
	Data Protection Officer		
SIRO escalation		For High Risks only	
	Senior Information Risk Owner (SIRO)		

Section 6 - Impact

Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: Staffordshire Police; the data subjects; and society/the general public

Describe the benefits and disadvantages to each of the above.

Staffordshire will benefit from this technology as it can carry out analysis of video/digital footage much faster and with additional capabilities that would be very time consuming to be completed manually (eg identify an individual in one piece of footage and then locate and identify where/when else they appear within the wider mass uploaded footage)

This will greatly benefit the force by being much more effective and efficient in our investigative approach to this [REDACTED]. This will allow the SIO to present to CPS and the courts through subsequent prosecutions, swifter identification of unknown offenders and also better understanding and presentation of the scale of [REDACTED]

Phase 2 relates to an extended pilot of [REDACTED] for a further trial running until [REDACTED] with [REDACTED] from across the Force being trained and licenced to use the software. The extended pilot aims to support the wider force to [REDACTED]

Section 7 - Information Lifecycle

7.1 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.

This information will be then be [REDACTED]
Once the trial has been completed, [REDACTED]
The system only produces flags for existing evidence to be used – such as a time marker for a still from [REDACTED]
Stills are produced from [REDACTED] These stills will be removed from [REDACTED] and then exist on [REDACTED]. Stills will be used in the same way as we would outside of [REDACTED]

Phase 2 – [REDACTED] Officers requesting images to be processed in [REDACTED]. The users cover the following areas – [REDACTED]. A standardised [REDACTED] will be required to confirm what area the request has come from to [REDACTED]. The user will then send a [REDACTED].

7.2 Provide a full description of the information lifecycle

Stage of Processing	Description
Collection Where does the data originate from, who will collect it, how will it be data obtained and how often?	From [REDACTED] and [REDACTED] 1) All [REDACTED] 2) A similar [REDACTED] will be conducted for [REDACTED], with custody images that date back up to [REDACTED] 3) [REDACTED] footage from [REDACTED] uploaded by [REDACTED], throughout the trial.

Further notes from point 1 & 2

Note around [REDACTED] data and [REDACTED] data:

- [REDACTED] was populated from Crime, Intelligence etc.
[REDACTED] However, [REDACTED]
images were used as a source to populate nominals (people) on
[REDACTED] based on their [REDACTED]
2. [REDACTED] was populated with the latest [REDACTED] custody image for
the [REDACTED]

5. There will be some duplication of images across the [REDACTED] and
[REDACTED] whilst the [REDACTED] data will also provide images
not uploaded to [REDACTED] will obviously contain more
recent images since [REDACTED]

Also please note that user will just search on [REDACTED]
and then if no matches search [REDACTED]

Phase 2 –

**Facial Image Acquisition Request – Completed by
OIC**

RFR can utilise both [REDACTED] For
the purposes of Phase 2 this will be [REDACTED]
Images will need to be saved in [REDACTED]

[REDACTED] The location of the original
footage will need to be recorded on the [REDACTED]

[REDACTED] including the image to be completed by
the OIC requesting the search and sent to [REDACTED]

	[REDACTED] [REDACTED] Please refer to [REDACTED] for further detail. [REDACTED]
Storage Describe where and how the data is to be stored	The [REDACTED] for image and video files. These will also [REDACTED] [REDACTED] Phase 2 Enrolment and Detection - [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	[REDACTED] [REDACTED] - all videos will be downloaded from [REDACTED] Access will just be for those [REDACTED] [REDACTED] The [REDACTED] who will require access to [REDACTED] to download videos relating to the [REDACTED] are (for an audit purposes) listed below. The download of videos will start when [REDACTED] are on site for the training and complete at the end of the trial.

	Phase 2 – The nd are as below:
Access Describe who has access to the data throughout the life of the processing	Phase 2 – the
Recording Describe the processes for recording the data	
Processors Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?	
Sharing With which external organisation(s) is the data shared, what data is shared, and why?	

Describe any sharing that will occur within Staffordshire Police. Outline any national and international sharing or processing.	Phase 2 – The OIC will send in a completed OIC will be provided report detailing results of facial search along with interpretation of results and advised further action.
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate	Once the trial has been completed, Phase 2 -
Disposal Describe the process for disposal of data, including when and how.	
7.3 Assets Describe the assets that you intend to use.	
Hardware	
Software	
Networks	
Hardcopy/paper	
Any other relevant assets	

Section 8 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

8.1 Do you intend to consult data subjects?

☐ **Yes**

If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.

☒ **No**

If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.

This is part of the [REDACTED] investigation.

The information held in the FR system would include first name and last name at minimum, plus any other information the Force would like to add as part of the enrolment, which includes phase 2.

Phase 2 will also include - [REDACTED]

8.2 Consultation Action Log

Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- | | |
|---|---|
| <ul style="list-style-type: none">• Data subjects• The general public• Union representatives• Information Security• DPO | <ul style="list-style-type: none">• Staffordshire Police Legal• [REDACTED]• Data processors• Information Commissioner's Office (ICO) |
|---|---|

Who	When	How	Outcome
DPO	[REDACTED]	Email / weekly meetings	Aware
Info sec	[REDACTED]	Email / weekly meetings	Aware
Unison	[REDACTED]	Email	Aware
Police Fed	[REDACTED]	Email	Aware

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10 i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

**** Please refer to Appendix A – Calculation of Risk or DPIA Guidance Document for matrix used when identifying Risk Scores.**

Examples of **risks to individuals** include:

- Discrimination
- Identity theft
- Financial loss
- Reputational damage or embarrassment
- Physical harm
- Wrongful arrest or prosecution
- Loss of confidentiality
- Inability to exercise rights

Examples of **corporate risks** include:

- Failure to protect the public
- Loss of public confidence
- Civil litigation
- Reputational damage
- Regulatory action
- Breaching other legal obligations

You should identify **solutions** such as:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Deciding not to collect certain types of data • Reducing the scope of processing | <ul style="list-style-type: none"> • Restricting access to data • Training staff to understand the risks |
|---|--|

- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct

- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful

- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation

- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation

- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy

- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention

- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Staffordshire Police systems if required?
- Is the retention period necessary and proportionate?

6. Security

- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights

- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to the DPO.

OFFICIAL-SENSITIVE

(Update when complete)

Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
	1 – Highly unlikely 2 – Unlikely 3 – Possible 4 – Likely 5 – Highly likely	1 – Negligible 2 – Minor 3 – Significant 4 – Major 5 – Severe	Very High High Medium Low Very Low	Describe the mitigation and whether it will be implemented	Is the risk: - Eliminated - Reduced - Accepted	Very High High Medium Low Very Low

OFFICIAL-SENSITIVE

(Update when complete)

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]		

				Produced by State Police for FBI [REDACTED]		
--	--	--	--	---	--	--

				[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		

9.2 Data Sharing - including the involvement of other Controllers and Processors							
- What contracts, MOUs etc are in place or may be required? - What measures have you taken place to ensure third parties comply with Data Protection laws? - What risks are involved with sharing data? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?							
Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk	
9.3 International Transfers							
- Will data be shared with a third party based outside the EU? - If you will be making transfers, how will you ensure that appropriate safeguards are put in place?							
Describe the source of risk and the nature of potential impact on individuals, include associated	Likelihood of	Severity of	Initial Risk	Mitigation/ Solution	Result	Residual Risk	

OFFICIAL-SENSITIVE

(Update when complete)

organisation/corporate risk and compliance risk	har m	har m				
9.4 Additional Risk Factors						
Describe any further risks, ensuring that any risks not already identified are included.						
Describe the source of risk and the nature of potential impact on individuals, include associated organisation/corporate risk and compliance risk	Lik elihood of har m	Seve rity of har m	Initial Risk	Mitigation/ Solution	Result	Resi dual Risk

OFFICIAL-SENSITIVE

(Update when complete)

[illegible]

				[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	

Section 10 – Operational Data Risks - Additional Risks Relevant to Operational Data Only

This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**

10.1 Data Logging

Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

If the data is processed electronically then will a log be retained of the following actions:

- **Collection**
- **Alteration**
- **Consultation**
- **Disclosure**
- **Combination**
- **Erasure**

- ☐ Yes
☒ No*
☐ Not applicable

*If you answered "no" then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
[REDACTED]	■	■	■	[REDACTED]	■	
[REDACTED]	■	■	■	[REDACTED]	■	

10.2 Data Categorisation

When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.

OFFICIAL-SENSITIVE

(Update when complete)

Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:						
• Suspected of having committed, or are about to commit, a criminal offence • Convicted of a criminal offence, • Victims of a criminal offence, • Witnesses to a criminal offence.				☐ Yes ☐ No* ☐ Not applicable If you answered "no" then you must record this as a risk below.		
Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk

DPO USE ONLY			
Section 11 – Outcome and Review			
11.1 Outcome			
Item	Name	Date	Notes
Residual risks approved by:			
DPO advice provided by:			
Summary of DPO advice, including whether the ICO must be consulted:			
11.2 Review			
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.			

OFFICIAL-SENSITIVE

(Update when complete)

OFFICIAL-SENSITIVE

(Update when complete)

Outline:	• The frequency of review
• Who will be responsible for reviewing the processing	• The date of the next review

11.3 Conclusions**DDPO Conclusions:**

Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with the DPA2018. Includes references to any changes that were introduced as a result of the DPIA process.

ISO Conclusions:

Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with Information Security Requirements. Includes references to any changes that were introduced as a result of the DPIA process.

DPO Conclusions:

Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with Data Protection Act 2018 and risks to Staffordshire Police. Includes references to any changes that were introduced as a result of the DPIA process.

OFFICIAL-SENSITIVE

(Update when complete)

OFFICIAL-SENSITIVE
(Update when complete)



Produced by Staffordshire
for FOI 21201

OFFICIAL-SENSITIVE
(Update when complete)

Appendix A – Calculation of Risk

Calculation of Risk

The risk value shall be calculated by multiplying the impact and likelihood figures together. This score will then indicate the severity of the risk.

For example:

(Likelihood) **3** x (Impact) **5** = Risk value of **15**

Likelihood	5	5 Low	10 Medium	15 High	20 Very High	25 Very High
	4	4 Low	8 Medium	12 Medium	16 High	20 Very High
	3	3 Low	6 Medium	9 Medium	12 Medium	15 High
	2	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
	1	1 Very Low	2 Very Low	3 Low	4 Low	5 Low
		1	2	3	4	5
Impact						

Likelihood score

Score	Probability		Description
	%	Timeframe	
1. Highly unlikely	0 to 5% chance	1 in 10 years or more	Not foreseen to occur
2. Unlikely	>5 to 10% chance	1 in 5 years	May occur in exceptional circumstances
3. Possible	>10 to 20% chance	1 in 1 year	Realistic chance of occurring
4. Likely	>20 to 50% chance	1 in 6 months	Will probably occur
5. Highly Likely	>50% chance	1 in 3 months or less	Expected to occur or occurs regularly

OFFICIAL-SENSITIVE
(Update when complete)

Impact Score

Score	Financial/other enablers	Operational	Public Confidence/Reputational
1. Negligible	0 to <0.1% of budget/cost savings and/or Negligible impact on modern policing key activity delivery	0 to 0.5% shift in key: 1. Early Intervention measures 2. Supporting victims and witness measures 3. Managing offenders measures and/or Negligible impact on key operational activity delivery	0 to 0.5% shift in: 1. Levels of Satisfaction 2. Feelings of safety 3. Fair and respectful treatment and/or Low level localised media interest and/or Minor impact on key public confidence activity delivery
2. Minor	>0.1 to 0.5% of budget/cost savings and/or Minor impact on modern policing key activity delivery	>0.5 to 2.5% shift in key: 1. Early Intervention measures 2. Supporting victims and witness measures 3. Managing offenders measures and/or Minor impact on key operational activity delivery	>0.5 to 2.5% shift in: 1. Levels of Satisfaction 2. Feelings of safety 3. Fair and respectful treatment and/or No external reputational impact and/or Negligible impact on key public confidence activity delivery
3. Significant	>0.5 to 2% of budget/cost savings and/or Significant impact on modern policing key activity delivery	>0.25 to 5% shift in key: 1. Early Intervention measures 2. Supporting victims and witness measures 3. Managing offenders measures and/or	>0.25 to 5% shift in: 1. Levels of Satisfaction 2. Feelings of safety 3. Fair and respectful treatment and/or Some negative regional media coverage or public/political concern and/or Significant impact on key public confidence activity delivery

OFFICIAL-SENSITIVE

(Update when complete)

		Significant impact on key operational activity delivery	
4. Major	>2 to 4% of budget/cost savings and/or Major impact on modern policing key activity delivery	>5 to 10% shift in key: 1. Early Intervention measures 2. Supporting victims and witness measures 3. Managing offenders measures and/or Major impact on key operational activity delivery	>5 to 10% shift in: 1. Levels of Satisfaction 2. Feelings of safety 3. Fair and respectful treatment and/or 1. Long term regional media coverage or public/political concern 2. Limited national media coverage or public/political concern and/or Major impact on key public confidence activity delivery
5. Severe	>4% of budget/cost savings and/or Severe impact on modern policing key activity delivery	>10% shift in key: 1. Early Intervention measures 2. Supporting victims and witness measures 3. Managing offenders measures and/or Severe impact on key operational activity delivery	>10% shift in: 1. Levels of Satisfaction 2. Feelings of safety 3. Fair and respectful treatment and/or 1. Loss of credibility in organisation 2. International media coverage 3. Public enquiry and/or Severe impact on key public confidence activity delivery

OFFICIAL-SENSITIVE

(Update when complete)