



STAFFORDSHIRE
POLICE

Data Protection Impact Assessment

Kulpa

Stage 1

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 1 DPIA identifies the high level criteria that identify if further risk analysis is required.

The Project manager and Information Asset Owner will complete the stage 1 document and send to the Deputy Data Protection Officer (DDPO)

A decision will be made (after consultation with the Information Security Officer and / or the Data Protection Officer in the event of any ambiguity) on whether the Stage 2 DPIA has to be completed.

This Stage 1 DPIA should be completed at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into the project plan.

OFFICIAL-SENSITIVE
(Update when complete)

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.pnn.police.uk

Version	Version date	Requester of change	Summary of change(s)
V0.1	20.10.25		

DOCUMENT REFERENCES

Ref	Document Name	Version Number

OFFICIAL-SENSITIVE
(Update when complete)

DDPO Assessment		
DDPO Use Only		
A. DPIA part 2 is not mandatory.	☐	
B. DPIA part 2 is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA Part 2 will be required.	☐	
C. DPIA Part 2 is mandatory.	☒	
Publication Scheme		
Can this DPIA be uploaded to the Publication Scheme, if not give reasons why i.e. sensitive material included that could disrupt policing operations	☐	

Data Protection Impact Assessment (DPIA) Part 1	
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.	
Section 1 - Governance	
Project Proposal Name:	KULPA
Information Asset Owner:	
Project Manager/Lead:	

OFFICIAL-SENSITIVE
(Update when complete)

OFFICIAL-SENSITIVE
(Update when complete)

DPIA Coordinator:	
Date on which processing will commence:	20.10.25
Date submitted to DDPO:	06/11/25
Note: DDPO will give an initial response within 10 working days of receiving the completed form.	

Section 2 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

Kulpa is a new SaaS platform designed to empower victims and survivors, whilst also providing efficiency savings for policing. This in turn should reduce victim attrition and enable speedy justice.

The platform is made publicly available via a free mobile app and web-app and provides a safe space to upload and securely store evidence of an offence.

Then, if and when the person is ready, they can choose to report the offence via the app and share the evidence they have stored directly with the police.

The relevant police force will then receive this evidence on their kulpa Police Command and Control System (kPCC) tenant.

kulpa captures the available metadata associated with digital evidence at source, meaning its use should significantly reduce the need to download a victim's mobile phone or other mobile device.

In effect, it enables true selective extraction of only the relevant evidence, with the victim's privacy respected and protected.

To ensure that the data is secure, holds evidential weight and is legally admissible, kulpa retains two accreditations ISO/IEC 27001:2013 Information Security Management System and BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information.

The platform's automatically-populated PDF files mean that the evidence is immediately usable in an exhibited Criminal Procedure Rules (CPR) compliant format, suitable for onward transfer to the CPS for a charging decision, with minimal need for any manual processing by police officers.

Kulpa was conceptualised around a systematic process-based approach which would seek to ensure that, end-to-end, the needs and requirements of each stakeholder were fulfilled to the fullest extent possible. Doing so should enable more effective and more timely justice.

Improved justice serves to improve public trust and confidence and creates an effective deterrent against committing criminal acts.

All processing is consensual under the kulpa terms, justified and The Proof of Concept (PoC) (undertaken with [REDACTED]) demonstrated and evidenced that Kulpa could:

- (a) Improve victim experiences.
- (b) Save police time and/or money.
- (c) Get usable data/evidence through the system more quickly.

There is compelling evidence to suggest that kulpa can empower victims and will provide considerable opportunities for efficiency savings within police forces.

Kulpa's use in the PoC resulted in a significantly more efficient, suspect-focused police investigation.

The PoC recognised a few potential barriers rather than disadvantages, namely:

It was recognised that technology is a part of life, but it does not mean everybody understands it or is able to use it, so kulpa would likely not be able to reach or help everyone.

A representative from the Victims' Commissioner's Office suggested that this could be a valuable tool and presents real opportunities, but in order for the full potential to be reached, and to avoid victims being disappointed, it would need to be supported by Government, Policing and the wider justice system. Another support service echoed these comments suggesting that it would need to be supported by a culture shift in policing. Another suggested that restoring confidence in police would take a 'miracle' – but seeing positive results and success over time would be encouraging.

Groups recognised "education is power" and so kulpa would need to be spoken about if people were to benefit from it.

It should be explicitly noted that no policing data is being shared with or processed by the supplier (kulpa). Only data from the supplier (kulpa user data) is being shared with policing upon the user's explicit request and consent.

Kulpa is a game-changing, proven, fully accredited, SaaS IT platform that empowers victims and addresses the significant challenges of public trust and confidence.

A free public app encourages more victims to come forward, with a safe space to upload and secure evidence (photographs, videos, audio, messages, documents etc - all in a forensically compliant manner) and the freedom to then choose if and when to share and report.

When a user does choose to share their evidence, a subscribing Police Force receive the evidence on their dedicated tenanted Kulpa Police Command and Control system (kPCC) which will provide a fully CPR-compliant evidential package to enable an immediate, suspect-focused investigation, without the need to seize or download the victims mobile phone.

In summary, kulpa empowers victims to report in a way that enables policing to be more efficient and more effective; significantly improving the chances for justice.

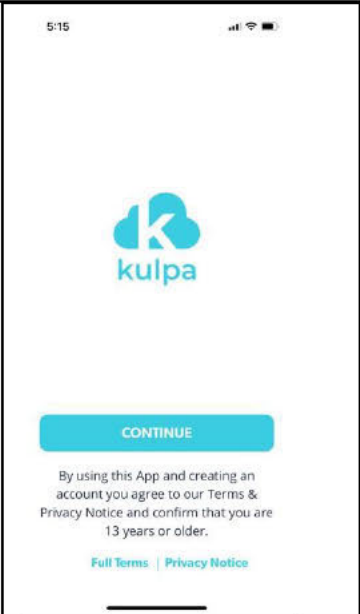
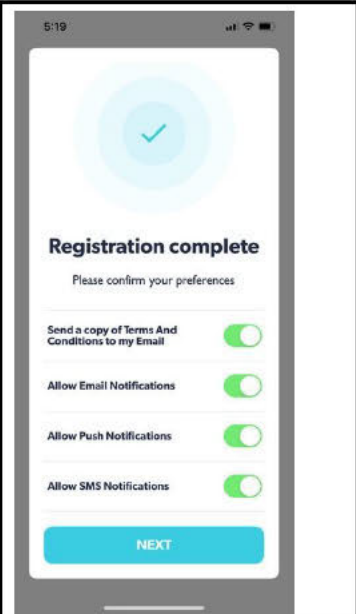
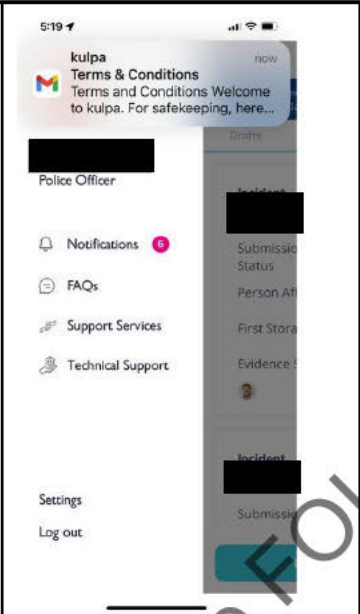
Following a very successful trial in [REDACTED] The Home Office's Accelerated Capability Environment (ACE), Police Digital Service (PDS) and Crown Prosecution Service (CPS), the kulpa solution was deemed by the PDS Digital Evidence Project (DEP) team to be suitable for deployment into policing.

A national pricing plan has since been agreed and the kulpa product (kPCC) can now be purchased by any UK police force and other law enforcement partners as a direct award call-off contract via kulpa's nominated reseller, Softcat plc, under an existing compliant public sector framework, HTE ComIT 2.

It is now proposed that the force purchase a kulpa SaaS subscription in order that it may receive digital evidence from members of the public who have captured and stored that evidence using kulpa.

Before using the kulpa platform (either the mobile app or web-app) the user must agree to kulpa's terms, conditions and privacy policy [1]. The acceptance of these terms means that the user has expressly given permission for data to be shared and processed by law enforcement.

OFFICIAL-SENSITIVE
(Update when complete)

			
App front login screen, stating that by using the app the user is agreeing to the privacy notice and terms. With direct links to said terms.	User can request a copy of the terms be sent to their email.	Copy of Terms is sent via email if the user chooses the option. Option is available each and every time the user logs in	

This consent is then re-affirmed twice more, at the point at which the user, presses the option 'share with police'.

Before sharing the data a 'check message' appears for the user which states

"Please confirm submission.

Once submitted the incident record and associated evidence will be sent to the relevant police force who will aim to contact you as soon as possible, taking note of your contact preferences.

Additional data and information can be added but submitted data cannot be amended or deleted.

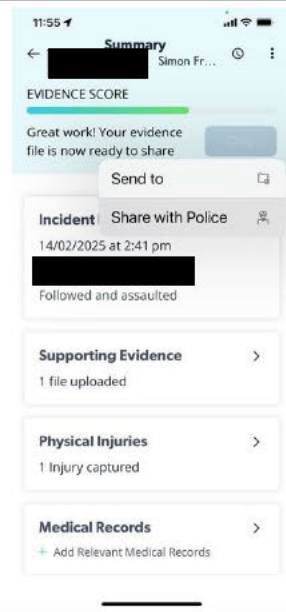
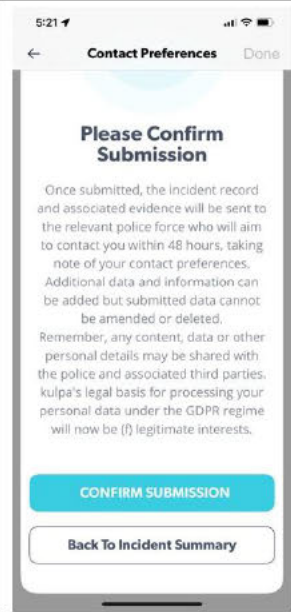
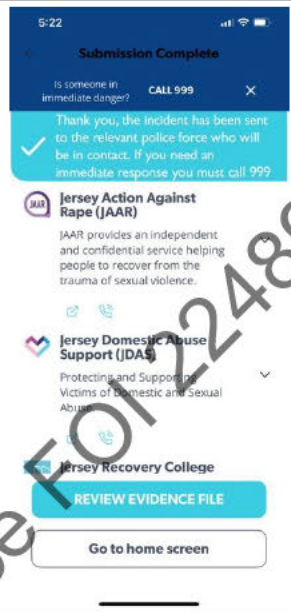
Remember, any content, data or other personal details may be shared with the police and associated third parties.

By submitting, you are confirming that the evidence is true to the best of your knowledge and belief and you share it knowing that, if it is tendered in evidence, you shall be liable to prosecution if you have wilfully shared, anything which you know to be false, or do not believe to be true.

kulpa's legal basis for processing your personal data under the GDPR regime will now be (f) legitimate interests.

Buttons

(CONFIRM SUBMUSSION)(Back to incident summary)

		
Options button, including 'share with police'	User given notice and required to 'confirm submission'	If confirmed case is submitted and guidance to local support services is provided

For the avoidance of any doubt, information shared by kulpa users with policing by selecting the option to 'share with police', will be received by the police force on their tenanted kulpa Police and Command Control System (kPCC). It is then for the reviewing officer / police staff to review the report, download the evidential package from the kPCC and upload it to the force RMS and DAMS systems. At this point, normal/standard processes, procedures and protocols continue.

It is essentially a new method for receiving an immediately usable package of digital evidence. No procedures or processes which follow are altered in any way. The information is uploaded to the existing RMS and DAMS. It is then on these systems which it is managed and shared onwards, for example to the CPS via TWIF (two-way interface). This is the interface police use to send evidence to the CPS for a charging decision and to exchange information thereafter. TWIF/EXISS2 is a two-way interface which allows CPS to send secure messages back. TWIF supports charging decisions being sent as structured data. Most other documents are sent as a set of Word docs or PDFs.

It is also perceived that officers will use the app to directly capture evidence at a crime scene, of both injuries of victims using the scaled images element of the app and also crime scenes photographs. This will standardise the capture of this evidence, and also save officer time with having to email and scale images as they will already be in the formats required for TWIF and DAMS and provide all the metadata and evidential trail requirements in forensic way.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

Personal data involved in this project will be that listed in the kulpa terms and privacy policy, which all users agree to before using the service.

<https://www.kulpacloud.com/termsAndConditions/Relative#policies>

PERSONAL INFORMATION WE COLLECT WHEN LOGGING INTO SYSTEM

When you download or use the platform, the categories of information that we may collect about you are as follows:

Personal information that you voluntarily give to us by entering information into or via the platform (including when registering to use the platform) and uploading content via the platform or otherwise and may include:

Name of person; *this includes victims and police officers name when logging in.*

Job title; *be completed on the MG11 Witness Statement which the system automatically populates. Such a statement should contain the witness occupation.*

Email address; *victims and police officers works email address.*

Address; *victims only not police officers stations.*

Contact telephone numbers; *victims and police officers work mobile phones.*

Date of Birth; *for both victims and police officers creating an account it is required to make sure person is over 18 and also to identify a person if wishing to delete an account in the future.*

Personally identifying information, data and files;

Medical information - *or user may photograph and upload a doctors letter, or they may screenshot or download data from the NHS app and upload it to kulpa as evidence would be at the users 'consent' given that they have to upload it*

Biometric data - *Users are required to take a photograph of themselves when opening a case file. Given that this image can "which allow or confirm the unique identification of that natural person" it is considered biometric. We request the image, 1 to humanise the report when it is received on the Kulpa police interface (kPCC) and secondly to ensure that we have evidence of who is in charge of the device at the time the evidence was uploaded (an important part of the evidential chain and validity)*

Information contained in our correspondence or other communications with you.

If you are a police officer we will also collect email address, collar/warrant number, police force and station;

If you are a medical professional we will also collect your medical number and practice details;

personal information about you that we may receive from the police or medical professionals;

information that we ask you to provide when you report a problem with the platform. If you

complete any surveys that we ask you complete for research purposes, we will collect information in

OFFICIAL-SENSITIVE
(Update when complete)

such circumstances as well, including your name, address, email address, phone number and enquiry details, which may include records of any correspondence and responses to any surveys; information that we collect about you and your Device, which we may do automatically. This includes (but is not limited to) weblogs, communication data, and the resources that you access. We may also automatically collect technical information, including anonymous data collected by the hosting server for statistical purposes, the Internet protocol (IP) address used to connect your computer/Device to the Internet, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, your Device IMEI and other technical information about your Device. We may also collect any personal information which you allow to be shared that is part of your public profile, time zone setting, browser plug-in types and versions, operating system and platform; and information that we collect about your location when using the platform (using GPS technology), where you have consented to the use of location services while using the platform.

UPDATED WITH CPS APPROVED LAYOUT

RESTRICTED (when complete) Case [REDACTED]

		MG11	
WITNESS STATEMENT			
Criminal Procedure Rules, r 27. 2; Criminal Justice Act 1967, s. 9; Magistrates' Courts Act 1980, s.5B			
Statement of	[REDACTED]	URN No.	
Age if under 18	Over 18	Occupation	CEO
This statement (consisting of 1 page(s)) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it, anything which I know to be false, or do not believe to be true.			
Signature	[REDACTED]	Date	04 March 2025, 09:39:17 AM
Electronically signed by [REDACTED]			
I am [REDACTED] I am making this statement in relation to an incident which occurred at [REDACTED] on 27 February 2025, 09:36:00 AM			

To assist, I produce as evidence, the following exhibits:

[REDACTED]	

There is no AI used in the creation of this statement.

2.3 Will special category data be used in the proposal? (Select all that apply)

OFFICIAL-SENSITIVE
(Update when complete)

OFFICIAL-SENSITIVE
(Update when complete)

- | | |
|---|--|
| ☒ Race | ☒ Trade union membership |
| ☒ Ethnic origin | ☒ Genetic Data |
| ☐ Political opinions | ☒ Biometric Data |
| ☒ Sex life | ☒ Sexual orientation |
| ☒ Religion | ☒ Health |
| ☒ Philosophical beliefs | ☐ None |

Other Notes:- Health

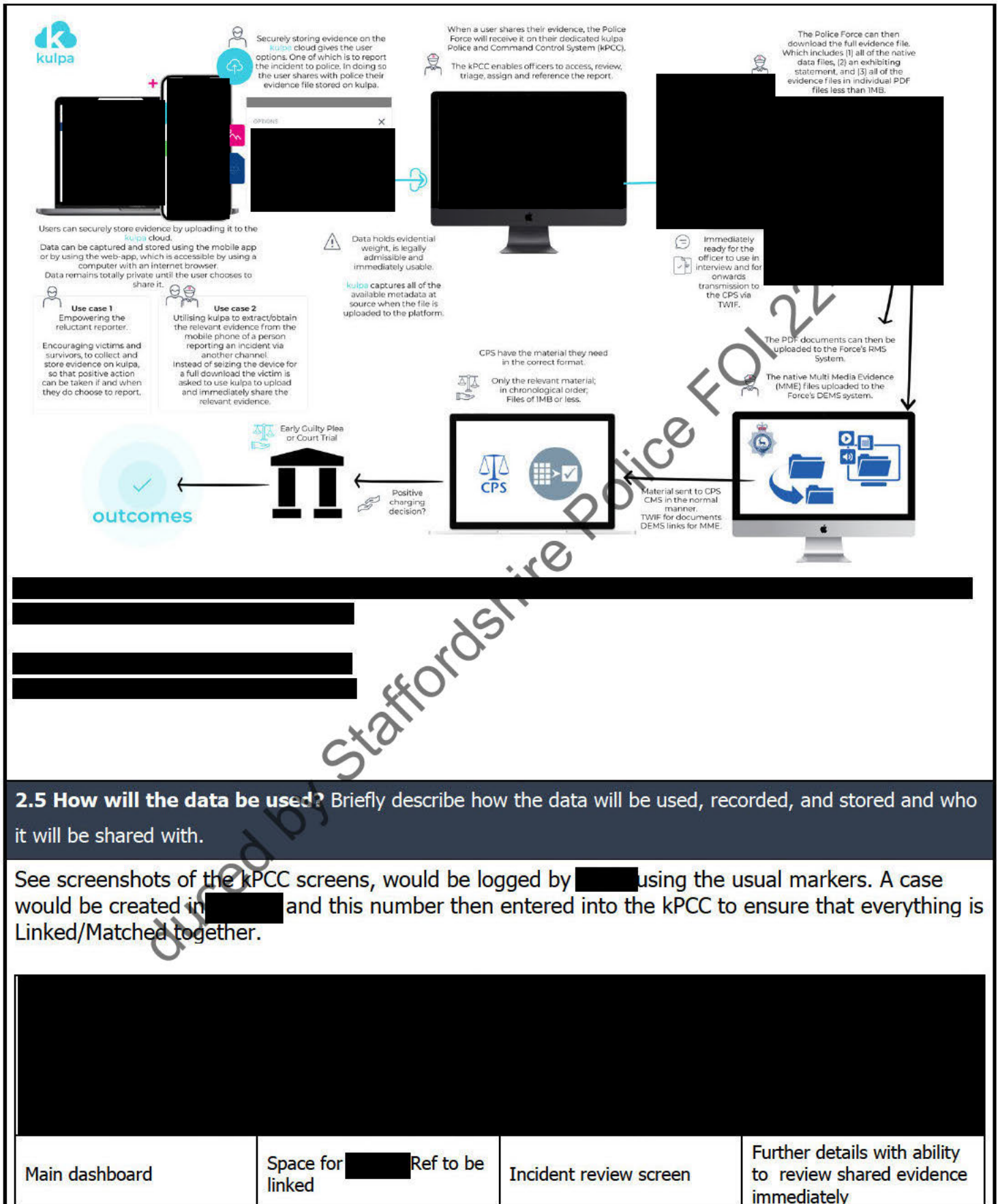
Users can store on the kulpa platform, data concerning their health in the form of any medical records relevant to the incident being reported.

Biometric data

In order to store evidence on the kulpa platform the user needs to provide a facial image which would constitute biometric data as defined in Article 4(14) that being "which allow or confirm the unique identification of that natural person"; whilst these activities are not presently performed on a large scale, as the platform grows it could be the case that a large scale of special categories of data is processed.

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in the Staffordshire Police's possession, from a different force.

OFFICIAL-SENSITIVE
(Update when complete)



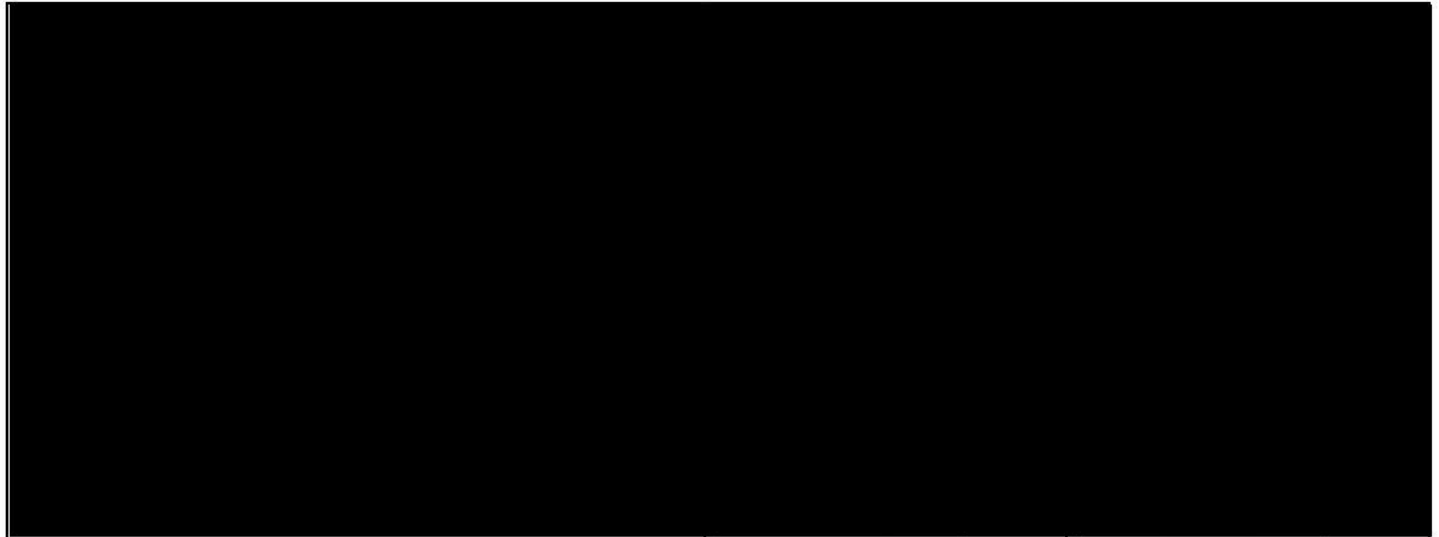
2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

See screenshots of the kPCC screens, would be logged by [redacted] using the usual markers. A case would be created in [redacted] and this number then entered into the kPCC to ensure that everything is Linked/Matched together.

Main dashboard	Space for [redacted] Ref to be linked	Incident review screen	Further details with ability to review shared evidence immediately
----------------	---------------------------------------	------------------------	--

The data provided from a kulpa submission will be used as evidence, to support an investigation of the reported incident and potentially a prosecution.

A reference number is entered by the reviewing police officer into the kPCC. [REDACTED] The kulpa user will then be able to see this reference, and their case will also turn blue on their app so that they know it has been reviewed. See attached screenshot. Further contact would be made through normal channels, phone, email, face to face.



Reference number entered on kPCC	Once a reference number is assigned the app displays a blue icon to the user	They can also via the app see the reference so that they can contact the force should they need to moving forward.
----------------------------------	--	--

Whilst the concept of kulpa is novel (it being a publicly available app), the technology used and processing is not novel. It is a data transfer of evidence and does not involve any other novel analysis or processing in the transaction between the kulpa platform (kPCC) and police systems.



Login screen to the kPCC	Example of audit trail which is accessible to all users.
--------------------------	--

Access to the kPCC is managed via the Forces own Single Sign-on (SSO) policies. The force therefore has full control over who can access the system, and ensures that access is provisioned and then de-provisioned when someone joins, moves or leaves.

Kulpa has a full audit trail of all activities

██████████ will only be able to see via our dedicated kPCC, the data which has been shared by a user reference a specific incident. ██████████ will not be able to see any information which has not been explicitly shared by a user and you will not be able to see shared data unless the incident being reported is within your force boundaries.

The Kulpa user can upload more data as and when they wish to do so. If they do this post a case already having been submitted then a message stating that further information has been uploaded will be sent to those using the kPCC within the force.

2.6 How many individuals will the processing affect? (Please specify one answer below)

- ☐ Fewer than 100 data subjects
- ☐ 100 to 1000 data subjects
- ☐ 1000 to 5000 data subjects
- ☒ More than 5000 data subjects

2.7 What categories of data subject are involved? (Please select all applicable categories below)

- ☒ Persons suspected of having committed or being about to commit a criminal offence
- ☒ Persons convicted of a criminal offence
- ☒ Persons who are or may be victims of a criminal offence
- ☒ Witnesses or other persons with information about offences
- ☒ Children or vulnerable individuals
- ☒ Staffordshire Police staff (current and former)
- ☐ Other

If other then please provide further details below:

2.8 Will it involve the collection of new information about individuals? Will Staffordshire Police collect data that it has not previously collected or had access to?

☒ Yes

☐ No

A free public mobile app, encourages more victims to come forward, with a safe space to upload and secure evidence (photographs, videos, audio, messages, documents etc - all in a forensically compliant manner) and the freedom to then choose if and when to share and report.

When a user does choose to share their evidence, a subscribing Police Force receive the evidence on their dedicated tenanted Kulpa Police Command and Control system (kPCC) which will provide a fully CPR-compliant evidential package to enable an immediate, suspect-focused investigation, without the need to seize or download the victims mobile phone

2.9 Data Sharing		Select one option
Does the processing involve:		
2.10.1	Data being shared with third parties external to Staffordshire Police or recipients that have not previously had routine access to the information?	☒ Yes ☐ No
2.10.2	Transferring data outside the UK but within the EU?	☐ Yes ☒ No
2.10.3	Transferring data outside the EU?	☐ Yes ☒ No
2.10.4	Storing data using a cloud service provider?	☒ Yes ☐ No
2.10.5	Is there an ISA, contract, or other sharing agreement in place with all parties with whom data will be shared?	☐ Yes – agreements in place ☐ Not yet – agreements required ☐ No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?

For example, can the aim be achieved by using less data or different types of data?

Are all categories of data necessary to achieve the aim?

Currently 77% of recorded Rape and other Serious Sexual Offences, Domestic Violence, Domestic Abuse, Stalking and Harassment offences cannot proceed due to an 'evidential difficulty' (Outcome 15 or 16). The use of the data from kulpa is fundamental in trying to reduce this percentage. Enabling victims and other members of the public to capture, store and then submit evidence to policing which holds evidential weight, and which is legally admissible. Only data categories and evidence which the kulpa user deems relevant and pertinent to the offence are received and processed.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

As outlined above,
'data subjects' have either directly consented to its use or are those accused of committing a crime.

Section 3 – Lawful Basis

3.1 Lawful Basis

To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Necessary for a law enforcement purpose

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes):

Necessary to protect the vital interests of the data subject or another person

3.2 Further Special Category Lawful Basis

If processing special category data (section 2.3) you must have identified a further lawful condition

Operational Data:

The processing is strictly necessary (please tick to confirm) ☐

AND

One of the following conditions applies (select from the list):

Safeguarding children and individuals at risk

Administrative Data:

It is necessary for one of the following conditions (select from the list):

Explicit consent

OR

It is in the substantial public interest (tick to confirm) ☐

AND for the following purpose:

Preventing or detecting unlawful acts and protecting the public against dishonesty, malpractice, unfitness or incompetence

Section 4 – Review, Retention and Disposal

4.1 Does the proposal have a review, retention and disposal process that complies with Staffordshire Police Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within the Staffordshire Police Retention and Disposal Schedule on the policy database.

Yes

Staffs Police all of the evidential packages obtained via the kulpa application are to be uploaded to the existing RMS and existing DAMS systems this is where they will be held for review and retention purposes. They will be retained and disclosed as per existing policies and procedures.

Staffs Police will follow CPIA guidelines and Forensic Science Regulator requirements with regards to data being processed and involved.

Kulpa will hold and retain data in line with its user terms and privacy policy. SoPs and accreditations kulpa has a full retention and disposal policy. Any data which is shared by Kulpa with police is retained for a minimum of 7 years within their system.

Section 5 – ICO: Additional Factors

OFFICIAL-SENSITIVE
(Update when complete)

The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.

Does the processing involve:		Please check either Yes or No	If 'Yes' then please provide further details
5.1	Systematic, extensive and large scale profiling and automated decision-making about people? <i>"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"</i> Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.	☐ Yes ☒ No	
5.2	Large scale use of special category data or criminal offence data? <i>"Processing on a large scale of special categories of data, or personal data relating</i>	☐ Yes ☒ No	

OFFICIAL-SENSITIVE
(Update when complete)

	<i>to criminal convictions and offences referred to in Article 10"</i>		
5.3	Public monitoring? <i>"Systematic monitoring of a publicly accessible area on a large scale"</i>	☐ Yes ☒ No	
5.4	New technologies or techniques? <i>"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"</i>	☐ Yes ☒ No	
5.5	Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? <i>"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"</i>	☐ Yes ☒ No	
5.6	Biometrics/genetic data? <i>"Any processing of biometric data" and/or "any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject" Biometric data can include Facial Recognition technology, fingerprints and is defined as</i>	☒ Yes ☐ No	The app uses facial ID to one the App for the user.
5.7	Data matching? <i>"Combining, comparing or matching personal data obtained from multiple sources"</i>	☐ Yes ☒ No	

OFFICIAL-SENSITIVE
(Update when complete)

5.8	Invisible processing? <i>"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"</i> For example, when gathering data, without the knowledge of the data subject, in the course of a Police investigation.	☐ Yes ☒ No	
5.9	Tracking? <i>"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"</i>	☐ Yes ☒ No	
5.10	Targeting of children or other vulnerable individuals? <i>"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children"</i> For example, the use of personal data relating to children for the purposes of marketing their online safety products.	☐ Yes ☒ No	
5.11	Risk of physical harm? <i>"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".</i> For example, if data relating to CSAE, HUMINT or protected persons data was	☐ Yes ☒ No	

OFFICIAL-SENSITIVE
(Update when complete)

	compromised then it could jeopardise the safety of individuals.		
5.12	Evaluation or scoring? <i>"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of a recruitment process.</i>	☐ Yes ☒ No	
5.13	Data processed on a large scale. <i>Considerations include:</i> • The number of data subjects concerned • Volume of data and/or range of data items • Duration, or permanence, of the data processing • Geographical extent of data processing	☐ Yes ☒ No	
5.14	Preventing data subjects from exercising a right? <i>The rights are:</i> • The right to be informed • The right to access data • The right to rectification • The right to erasure • The right to restrict processing • The right to object • The right to portability • Rights relating to automated processing	☐ Yes ☒ No	

Please forward the completed form the Staffordshire Police Deputy Data Protection Officer. SPDPO@staffordshire.pnn.police.uk.

OFFICIAL-SENSITIVE
(Update when complete)

Summary of Initial DDPO advice:

Additional advice from ISO and or DPO

Produced by Staffordshire Police FOI 22489