

2 March 2026

FOI Ref 22489

Request - You asked Staffordshire Police (SP) the following:

Please provide the following information held by your organisation in relation to the product known as "Kulpa", "Kulpa app", "Kulpa Police Platform" or "kPP", supplied by Kulpa Platforms Ltd (or any predecessor or related entity):

1. Confirmation of whether your organisation has entered into any contracts, trial agreements, memoranda of understanding, data-sharing agreements, or service orders relating to this product at any time from 1 January 2020 to the present.
2. For each such agreement, the start date, end date, and total contract value (or total amount paid).
3. The pricing model applied (e.g. fixed annual force-wide licence, per-user licence, per-case or per-incident pricing), and the number of user licences where this information is held.
4. Whether your organisation holds any business cases, Data Protection Impact Assessments (DPIAs), internal evaluations, or review reports relating to the adoption or use of Kulpa, and if so, copies of those documents with any necessary redactions applied.

SP received your request on 06/02/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

SP holds the requested information.

- 1. Confirmation of whether your organisation has entered into any contracts, trial agreements, memoranda of understanding, data-sharing agreements, or service orders relating to this product at any time from 1 January 2020 to the present. – **Disclosed, we have a trial agreement.**
- 2. For each such agreement, the start date, end date, and total contract value (or total amount paid). – **Disclosed, 1st November 2025 to 31st May 2026 cost £0.**
- 3. The pricing model applied (e.g. fixed annual force-wide licence, per-user licence, per-case or per-incident pricing), and the number of user licences where this information is held. – **Disclosed, No pricing model in place.**
- 4. Whether your organisation holds any business cases, Data Protection Impact Assessments (DPIAs), internal evaluations, or review reports relating to the adoption or use of Kulpa, and if so, copies of those documents with any necessary redactions applied. – **Partially disclosed, please see the accompanying files entitled 'FOI 22489 Certificate of Registration Evidential Weight', 'FOI 22489 Certificate of Registration Information Security Management', 'FOI 22489 DPIA Stage 1' and 'FOI 22489 DPIA Stage 2'.**



The following exemptions have been applied:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for this request.

- Section 40(2) Personal Information

Section 40(2) is an absolute exemption which means that there is no need to quantify the harm that may arise from the disclosure; neither is it subject to a public interest test.

To release personal or third-party information held by SP, would breach the data protection principles; namely –

- Data is lawfully and fairly processed.
- Processed in line with an individual's rights.
- Data is secure.

Personal and third-party information cannot be released under the Freedom of Information Act.

Disclosure under Freedom of Information is a release of information to the world in general and not an individual applicant.

- Section 24 (2) – National Security

Section 24 is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest.

Public Interest Test

Harm

Confirmation or denial that any further information is held relevant to this request would enable a geographical picture to be drawn up at force level, as well as a national level, about whether there are joint operational locations utilised and embedded by other law enforcement personnel; whether or not operating in concert with police officers of the host Constabulary. This would be vital police intelligence to individuals, some of whom may be terrorists or terrorist organisations, who are intent on targeting locations specifically utilised by Law Enforcement. Confirmation or denial that any other information is held would leave forces open to disruption and compromise the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending. Any disclosure that undermines the generic terms of duty of care provided by policing and Law Enforcement would be detrimental to the public at large. In short, any incident that results from confirming that any other information is or isn't held would by default affect National Security.

Factors favouring disclosure - Section 24

To confirm whether any other information is held relating to this request would better inform the general public as to the existence of policing and law enforcement capabilities within specific geographical locations. In turn, this can increase public confidence with the likely effect of dissuading mal-actors from operating within specific areas or regions.

Factors favouring non-disclosure - Section 24

Taking into account the current security climate within the United Kingdom, no information which may aid a terrorist should be disclosed.

Security measures are put in place to protect the community that we serve. To confirm whether any other information is held relevant to this request would provide a detailed account of the tactical infrastructure of not only a force area but also the country as a whole. This would highlight to terrorists and individuals intent on carrying out criminal or terrorist activity any vulnerabilities within the localities of specific forces. Confirmation, if held, would also allow inferences to be made about the nature and extent of national security related activities. This could enable terrorist groups to target sensitive police locations, and as such, confirmation or denial would be damaging to national security. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure both within the UK and Internationally.

Irrespective as to whether any information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain

Balance Test

When considering whether disclosure is appropriate, we must weigh the strongest reason for disclosure against the strongest reasons for non-disclosure. In this case, whilst the factors favouring disclosure are important in that it would adhere to the basic principle of being open and transparent, we believe when weighed against the risk of disclosure undermining our ability to prevent and detect crime and hindering our ability to protect the public, then non-disclosure takes precedence.

Please note that this data has been provided to the best of the ability of SP, subject to the limitation of current recording protocols and systems/software.

Please be advised that all Freedom of Information request responses are published on the SP website although personal details are not included.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from SP, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing within two months of the date of receipt of this email, and should be addressed to:

IAT@staffordshire.police.uk

Or by Post to:



STAFFORDSHIRE
POLICE

Information Access Team
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Information Access Team within two months of the SP response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing. The review will be conducted by a supervisor who is independent from the original Decision Maker. The Information Access Team will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within twenty working days. In more complex cases the review may take up to forty working days.

The independent supervisor will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, considering the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the independent supervisor will reply to the appellant with the result of the review. If the appellant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following link:
<https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Information Access Team