



STAFFORDSHIRE
POLICE

Our Ref: FOI 23175
Your Ref: FOI 23116

24th July 2026

Internal Review

Re: Request for internal review of response to application for information under the provisions of the Freedom of Information Act 2000, original request first notified to Staffordshire Police on 10th July 2026.

SP refers to the above request which was expressed in the following terms:

1. Yes or no - has your force shared intelligence with Horus Security Consultancy Ltd since February 2022?
2. If the answer Q1 is yes, has this included intelligence about:
 - a. Protest activity
 - b. Student protest activity
3. Yes or no - has your force received intelligence from Horus Security Consultancy Ltd since February 2022?
4. If the answer to Q3 is yes, has this included intelligence about:
 - a. Protest activity
 - b. Student protest activity
5. How much money have you paid Horus Security Consultancy Limited since February 2022, broken down by what services were paid for (e.g. insight intelligence services, DBS checks)?
6. Copies of any contracts you hold with Horus Security Consultancy Limited
7. Copies of any Information Sharing Agreements and Data Protection Impact Assessment you hold with Horus Security Consultancy Limited

Further to the above, SP also note the following comments made within your request for Internal Review.

Thank you for your response to my FOI request. I would be grateful if you could refer this case for an internal review.

I note that you have refused to confirm or deny whether the requested information is held, citing Section 31(3) of the FOI Act. This exemption is prejudice-based and requires a public authority to consider the extent to which confirming or denying would result in a real and significant likelihood of prejudice. The ICO advises authorities they must demonstrate “a ‘causal link’ between the disclosure and the prejudice claimed” and “show how disclosing the specific information requested would or would be likely to lead to the prejudice described”.

The refusal notice indicates that your police force is seeking to establish that the higher threshold of prejudice applies, stating that to disclose the requested information “would be likely to assist those seeking to understand, evade or disrupt police intelligence activity by identifying whether policing utilises information from the named organisation. Knowledge of the existence or absence of such a relationship may enable individuals or groups to adapt their behaviour with a view to limiting the effectiveness of intelligence-led policing activity, thereby prejudicing the prevention and detection of crime and the apprehension or prosecution of offenders.” The ICO has described this higher threshold as meaning the prejudice is “more probable than not” to occur.

This claim is clearly unsupported. To confirm or deny that the requested information is held would do nothing more than establish whether a commercial relationship exists between your police force and Horus Security Consultancy Limited. To do so would reveal no useful details about the products or services being provided or any operational capabilities. When the ICO considered a similar scenario in September 2018, in a case where a complainant had sought information about Bedfordshire Police’s Internet of Things capabilities (ref FS50739797), the Commissioner made a number of observations that are pertinent to this case.

In the Bedfordshire case, the Commissioner said: “Confirming that the requested information is held would disclose to the public that Bedfordshire Police holds information about its digital investigation and intelligence capabilities ... the Commissioner considers that, in the particular circumstances of the case, confirmation (if held) would not reveal something that is not already likely to be obvious to the public ... by confirming that it holds information about its digital investigatory capabilities, Bedfordshire Police would not be disclosing information about the extent of those capabilities.”.

In regards to what denying the information is held would reveal, the Commissioner added: “Turning to what denying that information is held would reveal, the Commissioner notes that Bedfordshire Police’s concern here is that it would suggest a vulnerability in the area of digital investigatory intelligence, which criminals could seek to exploit. However, as above, the Commissioner does not accept that it can necessarily be inferred from a police force’s denial that it holds information about its IoT.”

This position is supported further by an ICO ruling on a similar case in September 2025 (ref IC-399792-N9B7)], in which a complainant had sought substantially similar information about West Midlands Police’s relationship with Palantir Technologies UK Ltd. The requested information included Data Protection Impact Assessments and Information Sharing Agreements.

The Commissioner said that he was “not satisfied that West Midlands Police has demonstrated a realistic link between confirming/denying whether the requested information is held, and prejudice to the prevention or detection of crime, or the apprehension or prosecution of offenders. Such a link is not otherwise obvious to him. Consequently, he is not persuaded that merely confirming/denying would reveal any meaningful information about West Midlands Police’s investigative capabilities which would, or would be likely to, prejudice these law enforcement functions.”

He added that he was “not satisfied that simply confirming or denying whether such information is held would have the adverse effects that West Midlands Police has suggested. He considers its arguments on this point to be speculative. He is not satisfied that it has shown how or why confirming/denying would reveal vulnerabilities or operational information which could be exploited by hostile actors, to the detriment of national security.”

These arguments apply equally to my similar request for information on your use of Horus’ services, which would not reveal any material information about your operational capabilities. There is limited information in the public domain on the services Horus provides, other than that it offers a variety of open-source intelligence reports as well as DBS checks. As in the West Midlands Police case, the force acknowledged: “It is well established that police forces use publicly available data in order to counteract criminal behaviour.” The provision of DBS checks and open-source intelligence reports is not exclusive to Horus. Confirming or denying a commercial relationship with Horus in relation to one or both of these services would not materially assist potential criminals in evading detection.

Additionally, numerous other public bodies have disclosed their use of Horus’ services in response to Freedom of Information requests, including over a dozen universities such as King’s College London and the University of Bristol. This demonstrates that it is possible to confirm a commercial relationship without causing significant detriment to their law enforcement capabilities or ability to preserve health and safety.

Finally, you have given inadequate consideration to the public interest arguments in favour of disclosure, which vastly outweighs the speculative harms you’ve outlined. The use of Horus’ services by universities to monitor student activism has generated significant concern, in relation to individual right to privacy as well as the potential chilling effects on freedom of expression and assembly. There is an overwhelming interest in knowing whether other tax payer-funded bodies are using the companies services.

In sum, I request that you:

Conduct a review of the public interest test At a minimum, confirm or deny whether you hold the information Disclose the information covered under the scope of our request in full



STAFFORDSHIRE
POLICE

SP Response

Upon review of your request for information under the Freedom of Information provision referenced above, SP are of the opinion that the response issued fully answers the terms of your request.

We also confirm that the application of the exemption outlined within this response is fully justified, and that the explanation and rationale for its' application conveyed clearly and unequivocally.

If you are not content with the outcome of the review, you may apply directly to the Information Commissioner to investigate. The Information Commissioner can be contacted at:

<https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Information Access Team Management

IAT@staffordshire.police.uk