

Our Ref: FOI 22214
Your Ref: FOI 21836
Date: 16 December 2025

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 09/09/2025.

We refer to the above request which was expressed in the following terms:

Under the Freedom of Information Act 2000, I am writing to ask that you provide me with the following information on your use of mobile phone data extraction:

1. Does your police force currently carry out mobile phone data extraction in low level crime cases using self-service / downloading kiosks? Please provide your definition of low-level crime.
2. Does your police force currently carry out mobile phone data extraction in serious crimes using self-service / downloading kiosks?
3. If your police force is not currently using mobile phone extraction kiosks, have you trialled this in the past/do you have plans to in the future?
4. Does your police force currently use Hubs to carry out mobile phone data extraction in (a) low-level crimes? (b) serious crimes?
5. Do you centrally record mobile phone data extracted from kiosks?
6. If you have a mobile phone extraction kiosk, please provide the name of the company(ies) which currently provide(s) the hardware / software / to whom you pay a license for the relevant tools. If contracts for these tools exist, please also provide the beginning and end dates of these.
7. Does your police force use analytics software to process, analyse or evaluate data extracted from mobile phones? If so, please provide the name of the software or provider.
8. How many officers currently carry mobile phone examination kits on patrol and/or in vehicles and/or for other operational use in (a) low level crimes? (b) serious crimes?
9. Please confirm whether or not a review has been conducted into the use of self-service kiosks.
10. Please provide copies of the current relevant force level and/or national level guidance for the use of downloading kiosks.
11. Please provide copies of the current relevant force level and/or national level policy for the use of downloading kiosks.

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

I am contacting you in regards to your response to my FOI request on 'Use of Mobile Phone Data Extraction'.

Your response cited Section 24 (National Security) and Section 31 (Law Enforcement). As both exemptions are qualified exemptions, you are required to demonstrate that the disclosure would be likely to cause specific, identifiable prejudice, and that the public interest in maintaining the exemption outweighs the public interest in disclosure. I do not believe the response meets these statutory requirements.

The public interest test has not been adequately evidenced - as the test presented does not appear to be balanced. There seems to have been an inflated idea of how knowledge of the companies used would aid in criminal activity, or activity that could threaten national security.

There also has not been a consideration of a partial disclosure, e.g. disclosing the company but not the specific system or technology used.

I am therefore requesting a full internal review of the handling of my request.

Our Response

Having reviewed our initial response, we now issue a revision to this, please see below for our revised response.

The rationale for the PIT applied has been reviewed and our stance with regard to the application of exemptions under section 24 and 31 remains the same. We also confirm that the application of the exemptions outlined within this response are fully justified, and that the explanations and rationale for their application conveyed clearly and unequivocally.

- Under the Freedom of Information Act 2000, I am writing to ask that you provide me with the following information on your use of mobile phone data extraction:
- 1. Does your police force currently carry out mobile phone data extraction in low level crime cases using self-service / downloading kiosks? Please provide your definition of low-level crime.
– **Disclosed, yes. Low Level Crime would be defined as less serious in nature involving minimal harm and not a threat to public safety.**
- 2. Does your police force currently carry out mobile phone data extraction in serious crimes using self-service / downloading kiosks? – **Disclosed, occasionally if the requested data can be obtained.**
- 3. If your police force is not currently using mobile phone extraction kiosks, have you trialled this in the past/do you have plans to in the future? – **Not applicable.**
- 4. Does your police force currently use Hubs to carry out mobile phone data extraction in (a) low-level crimes? (b) serious crimes? – **Disclosed, a) Yes and b) Occasionally.**
- 5. Do you centrally record mobile phone data extracted from kiosks? – **Disclosed, no.**
- 6. If you have a mobile phone extraction kiosk, please provide the name of the company(ies) which currently provide(s) the hardware / software / to whom you pay a license for the relevant tools. If contracts for these tools exist, please also provide the beginning and end dates of these.

– Withheld, please see the below exemptions.

- 7. Does your police force use analytics software to process, analyse or evaluate data extracted from mobile phones? If so, please provide the name of the software or provider. – **No**
- 8. How many officers currently carry mobile phone examination kits on patrol and/or in vehicles and/or for other operational use in (a) low level crimes? (b) serious crimes? – **Disclosed, nil for both.**
- 9. Please confirm whether or not a review has been conducted into the use of self-service kiosks. – **Disclosed, yes.**
- 10. Please provide copies of the current relevant force level and/or national level guidance for the use of downloading kiosks. – **Withheld, please see below.**
- 11. Please provide copies of the current relevant force level and/or national level policy for the use of downloading kiosks. – **Withheld, please see below.**

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 parts of this particular request.

- Section 21(1) - Information reasonably accessible by other means.

Section 21 is an absolute, class-based exemption and as such there is no requirement to quantify the harm that may arise from the disclosure, nor is there a requirement to perform a Public Interest Test.

- Section 24 (1) – 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.

- Section 31 (1)(a)(b) Law Enforcement

Information is exempt from disclosure under S31 (1) (a) (b) where the release of Information would, or would likely to, prejudice the prevention and detection of crime and/ or the apprehension or prosecution of offenders. This exemption is qualified and prejudice-based and, as such, we are required to evidence the harm in disclosure and apply the public interest test.

Harm:

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, disclosure of a particular policing tool of this type is used by Staffordshire Police as part of an investigative process would reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of Staffordshire Police and others to safeguard national security.

It is well established that police forces utilise Digital Forensic techniques in order to counteract criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders. Modern day policing is intelligence led, and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to a service provider and by extension their products for the extraction of data from devices to their Kiosks.

By disclosing if Staffordshire Police use named software to process, analyse or evaluate data extracted from mobile phones such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force-by-Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Equally, given the sensitive areas in which tools of this type may be used, such as counter-terror investigations, to disclose if any particular tools are used would allow criminals and other adversaries to focus on evaluating the particular capabilities of its use. With this knowledge it would allow criminals and other adversaries to take steps to counteract a specific tool – be it adjusting how they interact and present themselves to take advantage of any weaknesses or gaps in capability they identify. For example, at a simple level, if a policing tool doesn't search 'X' social media site or was unable to identify 'Y' format of images and criminals can establish this, they will exploit this position. Staffordshire Police's more sophisticated adversaries may be able to go further and take more proactive measures to undermine the tool and/or its provider, and a specific confirmation allows efforts to be focused accordingly.

This detrimental effect is increased if the request is made to several different law enforcement bodies such as this request has. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to 'map' where the use of certain tools are or are not used. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Public Interest Test

Factors favouring disclosure under Section 24

Disclosing would provide the public with information about technologies and Staffordshire Police's capabilities. This would reinforce the wider commitment to openness and transparency with the general public and facilitate public debate. Furthermore, owing to the inherent link between transparency and public confidence, Disclosing the software name and how it works would be likely to improve the general public's confidence in Staffordshire Police. Over time, an increase in public confidence would be likely to improve public engagement with the police. This would, in turn, lead to an improvement in our ability to both prevent and detect crime, and apprehend and prosecute offenders.

Factors favouring non-disclosure under Section 24

Security measures are put in place to protect the community that we serve. To disclose the software name and its uses would be useful intelligence to terrorists and individuals intent on carrying out criminal activity.

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. The cumulative effect of those with ill-intent gathering information about force capabilities, would have greater impact when linked to other information gathered from various sources. The more information that is disclosed over time will provide a detailed account of the tactical infrastructure, not only at force level but across the country as a whole. Any incident that results from confirming that any information is held would by default affect National Security.

Factors favouring disclosure under Section 31(1)(a)(b)

The public have a genuine interest in what the police do and how they do it. Their interest is legitimate and to be encouraged within a democratic society where policing is by consent.

Public accountability for the use of resources and taxpayers' money, and a willingness to be transparent and open are desirable characteristics in all public authorities.

The interest on which software packages are being used and how is therefore to be expected, especially when there is some concern as to whether such expenditure is appropriate and justified.

Factors favouring non-disclosure under Section 31(1)(a)(b)

To disclose the particular software used and how it is used by policing would compromise the forces' ability to protect the public. Disclosing Staffordshire Police's capabilities would provide persons intent on disrupting their work, with information that would assist them to do so. In this case, for the reasons outlined in the evidenced harm, the effectiveness of current and future strategies when carrying out investigations and gathering evidence may be compromised. The safety of the public is of paramount importance to policing purposes, and any increase in crime would place the public at risk of harm. When the current or future law enforcement role of the force may be compromised by the release of information, the effectiveness of the force will be reduced.

The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, disclosing tactical information relating to the extraction of data from mobile devices, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

Balance test

The points above highlight the merits of disclosure and also non-disclosure. Having considered the reasons why Staffordshire Police should opt to not disclose the software name and its uses, although openness and transparency is at the forefront when considering the public interest, in this case disclosing the software used and how it is analysed, evaluated and used by the police for investigative purposes would not be in the public interest.

Whilst there is a public interest in appropriately and effectively engaging with the threat from criminals, there is a very strong public interest in safeguarding National Security. As much as there is a public interest in knowing that policing activity is appropriate and balanced in matters of National Security, this will only be overridden in exceptional circumstances.

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 any information that is released. Disclosing the software would reveal specific policing activity in the digital sphere of investigations and would assist those with intent on causing harm. Any incident that results from disclosure would, as a result, affect National Security.

We have found that disclosing the software used would directly harm the ability of Staffordshire Police to investigate crime. This could also reveal police capabilities, compromise police investigations and/or otherwise, adversely affect the ability of Staffordshire Police to safeguard national security. We have attached considerable weight to these interests as the primary role of the Police Service is to both prevent and detect crime and apprehend those responsible for committing criminal offences. Therefore, at this moment in time, there is no public interest in disclosing information that would increase the risk to public safety and harm policing capabilities.

Advice and assistance

In order to comply with our obligations under Section 16 of the Act, the obligation to provide advice and assistance, please find below links to the information requested within questions 10 & 11

[Extraction of material from digital devices | College of Policing](#)

Please be advised that all FOI requests and response letters are published on the Staffordshire Police website although personal details are not included.

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