



Your reference: N/A
Our reference: FOI_25_0229
E-mail: FOI
@gloucestershire.police.uk
Direct dial: 01452 754304
Postal Address: As above
Date: 24/04/2025

Dear

Gloucestershire Constabulary Freedom of Information request FOI_25_0229

On 24/02/2025 you sent an email constituting a request under the Freedom of Information Act asking the following:

I am requesting information regarding AI use in digital forensic departments nationwide. The questions relate only to your digital forensics departments, including units that process digital images, video and audio evidence. The responses given will be used in said dissertation to aid in my research.

The three questions for my research are:

1. Do any of your digital forensic departments employ tools/software that incorporate AI technology? This could include software that uses AI such as enhancement software or systems used for facial recognition.

If your response is "yes", then please include the name of the software(s) and details of what they used for.

2. What guidelines, regulations, or legislation do you follow in relation to AI use within your digital forensic departments?

3. Are there any AI tools/software that you plan on using in the near future?

Please do feel free to provide any further information you feel might be relevant regarding the use of AI within your digital forensics departments that are not covered within the questions above.

A PIT extension email was sent to you on 25/03/2025.

Under the Freedom of Information Act 2000 s1, I can confirm that Gloucestershire Constabulary holds some relevant information.

1. I can confirm that's Gloucestershire Constabulary does use some software tools to facilitate the processing of forensic images from computer devices.

The name of the software is exempt under virtue of Section 31 (1)(a)(b).

Section 17 of the Freedom of Information Act 2000 requires Gloucestershire Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states the fact, (b) specifies the exemption in question and (c) states (if not otherwise apparent) why the exemption applies.

The following exemption applies:

Section 31(1)(a)(b) – Law Enforcement

The exemption above is qualified and prejudice based therefore both a Public Interest Test and Harm Test are required.

Evidence of Harm

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

<https://www.app.college.police.uk/app-content/information-management/>

Commercial Forensic Service Providers and the software they offer are vitally important in the Criminal Justice system - not only do they play a crucial role by supporting UK Policing with backlogs in the Digital Forensics arena, but they provide Defence teams with access to independent forensic experts to support their clients.

Whilst not questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any digital forensic software used by the force would be extremely useful to those involved in criminality as it would enable them to create a map of tools and, by extension, providers most used by police Forces. Forensic Service Providers can, and have, be targeted by malicious actors. For example in 2019 Eurofins suffered a highly sophisticated ransomware attack which severely disrupted UK Policing and the Criminal Justice system.

Providing a list of digital forensics software used would mean that force by force, a criminal or individual with criminal intent could identify the software and/or providers most critical to law enforcement and specifically target those providing the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to cyberattacks which could have devastating consequences.

Public Interest Test:

Factors favouring Disclosure - Confirming details of the software used would be of interest to the public, namely give insight into the forensic processes used to solve crimes.

Factors favouring Non-Disclosure - Measures are put in place to protect the community we serve and as evidenced within the harm, to provide a detailed list of digital forensic software would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

Taking into account the current security climate and the increasing risk of cyber-attack within the United Kingdom, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

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

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. To provide the names of digital forensic software currently in use by the force increases the known risks of cyber-attacks and would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure.

2. All data is processed in accordance with the following guidelines, regulations or legislation of the following:

Data Protection Act 2018

The Extraction of Information from Electronic Devices: code of practice that relates to the exercise of powers in the Police

Crime Sentencing and Courts Act 2022

3. No

In accordance with the Act, this letter represents a Refusal Notice for this part of your request.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - <https://ico.org.uk/>

Call their helpline - 0303 123 1113

Email - casework@ico.org.uk

Post –

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Disclosure Officer
Gloucestershire Constabulary