

Date: 1st April 2025
Our ref: FOI/25/014289/T

FREEDOM OF INFORMATION REQUEST REFERENCE NO: FOI/25/014289/T

I write in connection with your request for information dated 25/02/2025, received by Greater Manchester Police (GMP) for the following information:

My name is [REDACTED], and I am a currently completing a Master's degree in Video & Audio Forensics at Liverpool John Moores University. 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.

Result of Searches

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP however, I am not obliged to provide all the information requested as exemption applies.

Question 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.

A. Yes

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

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

The information requested for the above part of question 1 is exempt from disclosure by virtue of the following exemption:

Section 31(1)(a)(b) – Law Enforcement

Section 31 is a qualified and prejudice based exemption and as such, subject to a harm and public interest test.

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.

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

The use of these tools are adopted for use align with our local policies.

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

No specific plans currently.