

Date: 02/12/2025
Our ref: 01/FOI/25/015655/Z

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/25/015655/Z

I write in connection with your request for information dated 13/10/2025, received by Greater Manchester Police (GMP) for the following information:

From 1 January 2017 to today, does Greater Manchester Police hold any licence, tenancy, or paid access (directly or via a supplier) to Relativity or RelativityOne for:

- *e-disclosure / e-discovery*
- *disclosure for major inquiries or criminal investigations*
- *Data Subject Access Requests (DSARs)*
- *Freedom of Information (FOI) review*

If so, please provide:

- a) whether access is direct or through a supplier (e.g., Epiq, Anexsys/Consilio, FTI, Deloitte, CCL)*
- b) contract reference(s)*
- c) the first start date and current status (active or expired)*
- d) whether the tooling is used for criminal matters, civil litigation, DSAR/FOI, or public inquiries*

If this information is held only in part, please provide the details that are available.

Result of Searches

Greater Manchester Police can neither confirm nor deny that it holds the information you requested as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of the following exemptions: **Section 24(2) – National Security** and **Section 31(3) – Law Enforcement**.

Harm – s24(2) and 31(3)

After careful consideration, GMP can neither confirm nor deny whether the requested information is held.

Any disclosure under Freedom of Information is a release to the public at large. Under the Act, we cannot, and do not request the motives of any application for information. We have no doubt that most requests made under the Act are legitimate and the applicants do not have any ulterior motives. Whilst not questioning the motives behind this specific request, confirming or denying whether RelativityOne is used would reveal details about the technological capabilities and security posture of GMP. This information could be exploited by hostile actors or organised crime groups to identify vulnerabilities, target specific systems, or develop countermeasures. Such knowledge could undermine national security by facilitating cyberattacks or compromising sensitive investigations that intersect with counter-terrorism or serious organised crime.

Confirming or denying whether RelativityOne, or other such systems, are in use could prejudice the prevention and detection of crime by indicating the technological capabilities available to GMP. Awareness of specific platforms could enable individuals' intent on criminal activity to adjust their methods (such as avoiding creating digital evidence that a system is designed to detect), exploit potential weaknesses in the platform, or attempt to compromise secure environments, such as crafted cyberattacks. This would risk undermining investigative effectiveness, jeopardise evidential integrity, and ultimately threaten the safety of victims, witnesses, and officers.

Confirming or denying whether this system is used would not only risk compromising the security posture of GMP but, when combined with responses from other forces, could create a mosaic of intelligence about law enforcement capabilities nationally. Adversaries could use this aggregated information to identify which forces employ certain technologies, infer operational strengths and weaknesses, and target specific systems or regions. This would prejudice the prevention and detection of crime, undermine investigative effectiveness, and increase the risk of cyberattacks and exploitation across multiple forces. For these reasons, maintaining a consistent Neither Confirm nor Deny position is essential to protect law enforcement operations and public safety.

Public Interest Test

Factors favouring Confirming or Denying for Section 24 - The information, if held, relates to national security and transparency could reassure the public that appropriate measures are in place. By confirming or denying if business is conducted with RelativityOne, or any other likeminded eDiscovery provider, would lead to a better-informed public.

Factors against Confirming or Denying for Section 24 - By confirming or denying whether any information is held would render policing and security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring Neither Confirming or Denying for Section 31 - Confirming or denying whether business is conducted with RelativityOne, or similar eDisclosure providers, could enhance public understanding of the Police Service's effectiveness and technology choices. Transparency in this area would help ensure accountability for public spending and demonstrate that resources are being used appropriately. It would also support informed public debate about law enforcement's digital capabilities, reducing speculation and misinformation.

Where significant investment in technology occurs, there is a legitimate public interest in knowing how funds are allocated and whether such tools contribute to operational efficiency.

Factors against Confirming or Denying for Section 31 - Confirming or denying whether any information is held regarding engagement with RelativityOne, or similar eDisclosure providers, would risk compromising law enforcement tactics and investigative processes. FOIA disclosures are monitored by individuals who are intent on criminal activity and hostile actors; therefore, acknowledging the use of specific platforms could provide insight into operational capabilities. This knowledge could enable adversaries to adapt their methods, exploit potential weaknesses, or attempt to compromise secure environments.

The Police Service relies on a range of techniques and technologies to gather intelligence and manage evidence, and revealing whether such tools are in use would prejudice the ability to prevent and detect crime. It could undermine investigations, increase the risk of cyberattacks, and ultimately place victims, witnesses, and officers at greater risk. Confirming or denying this information may also indicate relative vulnerabilities in law enforcement systems, which could be exploited to defeat security measures.

Public Interest Balance Test

The security of the country and the integrity of law enforcement operations are of paramount importance. GMP will not confirm or deny whether any information is held regarding business with RelativityOne, or any similar third-party provider, if doing so would place individuals at risk, undermine national security, or compromise policing tactics.

While there is a legitimate public interest in transparency around police technology choices and assurance that GMP is effectively addressing threats, this is outweighed by the very strong public interest in safeguarding investigative integrity and operational security across UK policing. Confirming or denying the existence of such information could reveal sensitive capabilities, expose vulnerabilities, and assist those intent on criminal activity or hostile acts.

Although the public has an interest in knowing that policing activity is appropriate and proportionate, this interest will only override operational security in exceptional circumstances. The use of technology in investigations is a sensitive matter, and disclosure—even by confirmation or denial—could prejudice law enforcement functions. Therefore, the balance of the public interest lies firmly in maintaining a Neither Confirm nor Deny position.

This should not be taken as indicating that any information meeting your request does or does not exist.