

Date: 05/06/2026
Our ref: 01/FOI/26/016859/I

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/26/016859/I

I write in connection with your request for information dated 11/05/2026, received by Greater Manchester Police (GMP) for the following information:

I am writing to make a request under the Freedom of Information Act 2000. I would be grateful if you could provide the following information relating to Greater Manchester Police's telephony and contact centre systems. Much of this information is available through looking at past tenders, but I would really appreciate a more thorough breakdown.

SECTION 1 — CORE TELEPHONY PLATFORM

Q1. *What telephony platform(s) does the force currently use? (e.g. Avaya, Mitel, Cisco, Microsoft Teams, other — please name the product and version where known)*

Q2. *Are these systems hosted on-premise, in a private cloud, or in a public cloud environment?*

Q3. *Who is the primary supplier/integrator responsible for delivering and supporting the telephony platform?*

Q4. *When do the contracts expire (month and year)? and are there plans for a new tender*

SECTION 2 — CONTACT CENTRE / 999 AND 101 HANDLING

Q5. *What platform is used for your force contact operations centre (handling 999 and 101 calls)? (e.g. Avaya Aura Contact Centre, Genesys, NICE CXone, other)*

Q6. What Session Border Controller (SBC) product is used to connect your SIP trunks to the public network? (e.g. Oracle/Acme Packet, Avaya SBCE, Cisco CUBE, AudioCodes)

Q7. What workforce management system is used (if any)?

Q8. What call recording system is in use within the contact centre?
(e.g. NICE, Verint, Redbox etc)

SECTION 3 — UNIFIED COMMUNICATIONS AND WIDER INFRASTRUCTURE

Q9. Does the force use Microsoft Teams for internal communications? If so, is Teams also used for any telephony (Direct Routing or Operator Connect)?

Q10. What Integrated Communications Control System (ICCS) is in use in the force control room? (e.g. Frequentis, Zetron, other)

Q11. What is the procurement route used for telephony and communications contracts? (e.g. Crown Commercial Service framework, direct award, open tender, regional collaboration)

SECTION 4 — REFRESH AND PIPELINE

Q12. Are there any active or planned procurements for replacement or upgrade of the telephony or contact centre platform in the next 24 months?

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, but I am not obliged to provide all of it as exemptions apply. Section 17 of the Freedom of Information Act 2000 requires GMP, when refusing to provide such information (because the 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 in questions 2, 5, 6 and 10 is exempt from disclosure by virtue of **Section 24(1) – National Security** and **Section 31(1)(a) - Law Enforcement**. There is a requirement to articulate the harm in disclosing such information as well as carrying out a public interest test for both exemptions.

S24(1) – S31(1) - Evidence of Harm

Every effort should be made to release information under Freedom of Information. However, a FOIA response is a release to the world as once the information is published the public authority have no control over what use is made of that information.

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. To achieve these objectives each force has a telephony and communications network infrastructure to support the vital information technology essential to front line services. Disclosure of specific IT and telephony services, capabilities,

or the lack thereof, in concert with any formal acknowledgement of strategic deficiency would reveal intricacies of those systems thereby highlighting vulnerabilities and compromising individual force information assurance.

As this request has been received nationally, disclosure would enable a geographical picture to be drawn up by those individuals who are intent on infiltrating or defeating police systems; some of these individuals may include terrorists or terrorist organisations. In terms of duty of care, this would be detrimental to the public at large as disclosure could assist a malicious actor by highlighting vulnerable forces and leaving those forces open to disruption of Information Technology or telephony systems; thus compromising the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending.

Public Interest Test

Factors favouring disclosure - Providing information in respect of GMP's network infrastructure would allow the public to be better informed on the health state and performance of said Information Technology and telephony platforms. In addition, forces are required to demonstrate efficient services to local taxpayers and satisfy audit requirements. This would provide transparency regarding the use of public funds in so much as highlighting that funds are being used to correctly and appropriately ensure all forces have adequate infrastructure, which results in the smooth running of force Technology systems.

Factors favouring non-disclosure - Whilst there is public interest in providing reassurance that police forces are appropriately and effectively dealing with any threats posed by terrorist organisations against police force Technology capabilities, there is a strong public interest in safeguarding National Security and the welfare and safety of the general public at large. Any disclosure has the potential to undermine current and future data integrity, which in turn compromises the force's mandate to protect the security of the United Kingdom, e.g. counter-terrorism activity. The risk of significant harm or even death to the community at large would be increased. Any disclosure of information that may lead to compromise of force IT and telephony systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism, is not in the interest of the public.

Balance Test

The security of the country is of paramount importance, and the Police service will not divulge any information if to do so would undermine law enforcement and therefore compromise the work of the police service. Whilst there is a public interest in the transparency of policing and force infrastructure, including any initiatives conducted with the private sector in relation to impacting on the crime or terrorist threat, there is a very strong public interest in safeguarding the integrity of these arrangements in this very sensitive area.

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater openness and transparency to the community at large with regard to the Information Technology resources available to the police, and whilst there is always a public interest in the transparency of how a police force delivers effective law enforcement and ensures the National Security of the United Kingdom is robust, there is a very strong public interest in safeguarding the intricacies and tactical capabilities of the systems used when dealing with information.

In every case, public safety is the paramount focus and any information which would place individuals at risk and compromise the National Security of the United Kingdom, no matter how generic, is not in the public interest. The effective delivery of operational law enforcement and the National Security of the United Kingdom is crucial and of paramount importance to every force. This would have a negative impact on law enforcement and national security

1. Avaya.
2. Exempt under s24 & S31, see above.
3. BT.
4. Contracts expire December 2028 –tender likely to take place late 2027 or early 2028.
5. Exempt under S24 & S31, See above.
6. Exempt under S24 & S31, see above.
7. Calabrio.
8. NICE.
9. Teams is used for internal communications, but not for telephony.
10. Exempt under S24 and S31, see above.
11. We use whichever route to market we believe will provide most competition and best value for GMP. So not necessarily fixed to any one route.
12. A procurement for Back-Office telephony has recently been run and awarded. We are currently considering our options over Contact Centre and may put out a pre-market engagement covering our requirements. Likely in the next month or so.