

Date: 13/07/2026
Our ref: 01/FOI/26/017126/I

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/26/017126/I

I write in connection with your request for information dated 25/06/2026, received by Greater Manchester Police (GMP) for the following information:

I'm carrying out research, which we intend to publish, into how UK public-sector organisations approach supplier information security. To that end, under the Freedom of Information Act 2000 I would be grateful for the following, regarding your procurement / supplier-onboarding processes:

- 1. Do you require suppliers (or prospective suppliers) to complete an information-security questionnaire or assessment as part of procurement, onboarding, or due diligence?***
- 2. If so, please provide a blank copy of the questionnaire(s) currently in use, noting any standard it references (e.g. Cyber Essentials, ISO/IEC 27001, NIST).***
- 3. Separately, do you require suppliers (or prospective suppliers) to hold Cyber Essentials, or an equivalent information-security certification, as a condition of doing business with you? If so, which certification(s)? (If this applies only in certain cases — for example above a contract-value threshold — a brief note is welcome, but not necessary.)***

I am requesting blank, standard templates only — not any completed questionnaire, supplier-specific information, or personal data. If any part would exceed the cost limit, please advise which part can be answered within it and treat that as my request. Please provide your response and any documents electronically, by email — I do not require paper copies. Thank you for your time.

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 supply all the information as exemption applies.

For question 2, GMP rely on the exemption under **Section 43(2) Commercial Interests** of the Freedom of Information Act 2000.

Section 43(2) is a qualified, prejudice-based exemption. This means GMP must demonstrate the specific commercial harm disclosure would cause. We must also apply the Public Interest Test to balance the public interest in disclosure against the public interest in withholding the information.

Harm

The information security assessments we use are uniquely tailored to each specific tender exercise. Releasing a blank questionnaire reveals our precise assessment methodology, evaluation scoring criteria, and technical thresholds to the public domain.

Future bidders could use this information to genericise or manipulate their submissions to match our specific scoring patterns rather than presenting their genuine capabilities. This distortion would severely undermine the fairness, competitiveness, and integrity of all future procurement exercises.

Disclosing these documents would give future suppliers an unfair commercial advantage over the police force during competitive negotiations. It would compromise our ability to obtain the best value for money from public funds during subsequent tender exercises.

Furthermore, releasing our internal security criteria allows malicious actors to map our technical vulnerabilities and security expectations.

Factors in Favour of Disclosure

Disclosure shows accountability regarding how the police force evaluates external suppliers and spends public money. Releasing the criteria demonstrates that the force robustly vets the information security standards of its third-party contractors.

Factors in Favour of against disclosure

There is a strong public interest in maintaining a fair, uncompromised, and fiercely competitive marketplace for public contracts. The public interest is best served when the police force can negotiate effectively to secure optimal value for the taxpayer.

Protecting the specific information security standards of GMP systems is vital to prevent cyber threats and safeguard public safety. Preventing future bidders from gaining an unfair tactical advantage ensures a level playing field for all commercial entities.

There is a critical public interest in ensuring our information-security checks remain rigorous, unpredictable, and capable of exposing weak supplier systems.

Cybercriminals could use these specific questionnaires to identify the exact technical limits, software requirements, and system boundaries used by GMP. This intelligence would allow hostile actors to launch highly targeted cyberattacks against both the force and our third-party supply chain.

Balance Test

We recognise that transparency in public procurement is highly important to the community. However, this transparency must be weighed against the severe risk of distorting commercial competition and compromising digital security. If suppliers can predict our exact security thresholds, the effectiveness of our vetting process drops significantly. We cannot compromise our ability to run thorough,

uncompromised information-security checks on companies handling police data. The public interest is best served by keeping our assessment tactics secure to protect GMP from exploitation.

Therefore, the public interest in maintaining the integrity of the tendering process, protecting police infrastructure, and safeguarding public funds outweighs the public interest in disclosing this information.

Please see the remaining information below.

Q1 – All tenders must comply with GMP's IT Security Policy. We also carry out additional security questions. These are not generic and are specific to each tender.

Q3 - Yes, where appropriate.