

Date: 18/08/2026
Our ref: 01/FOI/26/017238/P

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/26/017238/P

I write in connection with your request for information dated 14/07/2026, received by Greater Manchester Police (GMP) for the following information:

Under the Freedom of Information Act 2000, please provide the following about your printing/multifunction-device (MFD) provision. Please answer for each category: a) Photocopiers/MFDs, b) Desktop printers, c) Print room / reprographics.

Contract & supplier

- 1. Are you in contract for a managed print service? Is it fully outsourced?***
- 2. Who is the incumbent supplier for each category above?***
- 3. What is the manufacturer/brand of the devices (if different to Q2)?***
- 4. What is the contract start date and end date for each, and what extension options remain?***
- 5. How was it procured — direct award or mini-competition? If via a framework, which one (e.g. CCS RM6174, KCS, ESPO, YPO, NHS Supply Chain, NOE CPC, LPP)?***

Scale & spend

- 6. How many MFDs and how many printers do you have?***
- 7. What is the annual spend on the managed print service (lease, cost-per-click, consumables, service)?***
- 8. What are your annual print volumes (mono and colour)?***
- 9. How many sites/locations does the contract cover?***

Software & capability

- 10. What print-management software do you use (e.g. PaperCut, Equitrac, uniFLOW, YSoft SafeQ)?***
- 11. Do you have secure/follow-me print and mobile print capability?***
- 12. What device/fleet remote-monitoring software do you use?***

Renewal & ownership

13. Any planned procurement to replace or re-tender print/MFDs in the next 24 months? If so, when and via which framework?

14. What is the job title/role of the person responsible for the print estate, and the generic team contact for print procurement?

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 an exemption applies.

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.

Question 14 is exempted from disclosure under **Section 40(2) Personal Information** –Some information you have requested constitutes personal data of an identifiable living individual/s, and to disclose this information would breach the principles of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Personal data is defined by Section 1 of the Data Protection Act 2018 and means data that relates to an individual who can be identified directly or indirectly from that data.

Section 40 is an absolute exemption with no requirement to complete a public interest test.

In addition, the following exemptions are also engaged this time in relation to **question 12**.

The exemptions that apply to question 12 are:

Section 31 (1)(a)(b) Law enforcement

Section 24 (1) National Security

S31 Harm

The requested information relates to software used to remotely monitor, manage and maintain devices within GMP's ICT estate. Whilst the information may appear innocuous, disclosure would reveal details of the technologies used to oversee and support systems across the Force.

The disclosure of the specific software products in use would provide malicious actors with valuable intelligence regarding GMP's technical environment. Once a software product has been identified, extensive information regarding that product is often publicly available, including known vulnerabilities, exploit methodologies, configuration weaknesses and techniques designed to bypass monitoring mechanisms.

The crucial concern is that disclosure would assist individuals seeking to attack police systems by enabling them to build a clearer picture of GMP's technological infrastructure and security arrangements. Cyber criminals frequently seek to identify the monitoring, management and security tools deployed within an organisation before developing attack methods tailored to those technologies.

Furthermore, remote-monitoring software is rarely confined to a single service. Such solutions are routinely deployed across multiple systems and business areas. As a result, knowledge of the software used to manage one less sensitive area of GMP's estate could provide insight into the monitoring arrangements protecting critical operational systems. This information could be combined with other publicly available information to identify opportunities to gain unauthorised access, evade detection, disrupt services or compromise sensitive information.

Disclosure would therefore be likely to increase the risk of cyber-attack against GMP's networks and systems. Any successful attack could adversely affect policing operations, compromise sensitive information and undermine GMP's ability to prevent and detect crime.

Accordingly, disclosure would be likely to prejudice law enforcement functions and the prevention and detection of crime

S24 Harm

Police forces form part of the United Kingdom's Critical National Infrastructure landscape and work closely with national partners to protect the public from threats including terrorism, organised crime and cyber-attacks. Modern policing is heavily reliant upon secure and resilient technology systems.

The disclosure of detailed information regarding software used to monitor and manage devices across GMP's technology estate would reveal information about protective measures implemented to secure police systems. This information could potentially be exploited by individuals or groups seeking to undermine the security and resilience of those systems.

A compromise of police systems has the potential to affect operational policing capabilities, information sharing, investigative activity and wider national security interests. Whilst disclosure of this information alone may not cause such harm, it would contribute to the wider mosaic of information available to hostile actors and could assist in developing a more detailed understanding of police technological infrastructure.

For these reasons, disclosure would present a risk to national security interests.

S31 PIT

Factors Favouring Disclosure

Disclosure would promote openness and transparency regarding the technologies used by GMP.

Disclosure would improve public understanding of how public funds are spent on technology and ICT infrastructure. There is a public interest in understanding the measures GMP has in place to manage and monitor its devices and systems.

Disclosure may contribute to public confidence that appropriate technology solutions are being utilised to support policing functions.

Factors Favouring Maintaining the Exemption

There is a very strong public interest in protecting GMP's systems, networks and information assets from cyber threats and criminal attack. Disclosure would provide valuable intelligence to malicious actors regarding the technology deployed within GMP's environment.

Once the specific software products are identified, individuals could research publicly available information regarding vulnerabilities, exploits and methods of defeating or bypassing the software. The requested software forms part of GMP's broader monitoring and management infrastructure.

Disclosure concerning one area of the Force's environment could provide insight into the monitoring arrangements protecting more sensitive and operationally critical systems. The release of this information would increase the risk of unauthorised access, cyber-attack, disruption of services, compromise of police information and other criminal activity.

Any compromise of GMP's systems could adversely affect the Force's ability to prevent and detect crime, safeguard information and maintain operational effectiveness.

S24 PIT

Factors Favouring Disclosure

Disclosure would promote openness and accountability in relation to the technology used by GMP. There is a public interest in understanding how public authorities manage and secure their technological infrastructure. Disclosure would contribute to the transparency objectives of the Freedom of Information Act.

Factors Favouring Maintaining the Exemption

There is an exceptionally strong public interest in protecting national security and ensuring that policing infrastructure cannot be exploited by hostile actors. Police forces form part of the UK's wider law enforcement and national security framework and rely on secure information systems to support operational activities.

Disclosure would reveal information relating to the protective measures used within GMP's technology estate and contribute to a wider intelligence picture which could be used by individuals seeking to undermine those systems. Even seemingly limited technical information can have intelligence value when combined with other information already in the public domain.

Any successful compromise of police ICT systems could adversely impact operational policing, intelligence handling, public protection functions and wider national security interests. There is a strong public interest in ensuring that information which could assist hostile actors in identifying and exploiting weaknesses in policing infrastructure is not placed into the public domain.

Balance test.

There is a public interest in the disclosure of any systems used for this request, and although transparency is important, the integrity of law enforcement operations vastly outweighs the benefits of disclosure.

Revealing such information would increase the risk of crime, undermine operational policing and compromise the safety of major events.

Furthermore, disclosure of the requested information would meaningfully assist individuals seeking to compromise protective measure and exploit security systems.

Considering all the circumstances of this request, it is determined that the balance of the public interest favours withholding the information for these parts of the request.

Please see the remaining information for disclosure.

1. Yes.
2. Xerox
3. N/A
4. (MFD) - January 2019 and will be extended until December 2027.
5. MFD's RM3781.
6. We currently have 88 multi-function devices (MFDs) and 170 black-and-white/colour printers. In addition, there are five high-volume industrial printers, which are used by the Design and Print team and CTO. Our print room also has 2 Versant Printers supplied by Xerox.
7. £212.134.

8. The total print volumes comprised 2,680,038 black and white impressions, 3,522,709 black and white impressions produced on colour devices, and 1,974,422 colour impressions.
9. This currently covers 64 sites.
10. Ysoft SafeQ.
11. Follow me print.
12. See Exemption above.
13. The framework at this time is undecided however, a tender will be run in 2027.
14. See exemption above.