

Date: 06/05/2026
Our ref: 01/FOI/26/016759/F

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/26/016759/F

I write in connection with your request for information dated 23/04/2026, received by Greater Manchester Police (GMP) for the following information:

FOI Request 4: Vulnerability Flag Compliance

- 1. Provide details of the current procedure for flagging a caller's vulnerability status to attending officers prior to deployment.***
- 2. Confirm whether, on 12-04-2026 my registered vulnerability status was communicated to the attending officers. If not, fully and comprehensively explain the failure.***

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 some of the information requested is held by GMP.

The Freedom of Information Act provides the public with a general right of access to recorded information held by public authorities. However, information disclosed under this Act is effectively released into the public domain, or to the 'wider world', and not only to the person making the request. In cases where the public request information relating to individuals, it would be extremely rare for a public authority to release such information to the whole world under the terms of the Freedom of Information Act 2000.

Therefore, in accordance with the Act, this letter represents a refusal notice for **question 2** of this request.

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 exemption:

Section 40(5B)(a)(i) - Personal Information – giving information to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the principles of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

To confirm that any information is held or not, could confirm personal data. In some circumstances confirming or denying whether information is held could itself identify a living individual and would therefore breach the principles of the GDPR and the Data Protection Act 2018.

Personal data is defined by Article 4 of the GDPR and Part 1 of the Data Protection Act 2018, and means any information relating to an identified or identifiable natural person ('data subject'). An identified natural person is one who can be identified directly or indirectly from that data.

This use of neither confirm nor deny should not be taken as proof that such information does or does not exist.

Remaining response for question 1.

Identification of vulnerability is part of the THRIVE assessment as detailed in the incident response policy on the below link, as this identification would be based on the information gathered at the time of contact or based on known information / information obtained via police systems.

With regards to the vulnerability being communicated to attending officers, some information is passed via the air to the attending officers, however all officers are equipped with work issue devices that allow them to review the information from the incident etc and they have a responsibility to ensure they have the appropriate information prior to arriving on scene.

[incident-response-policy-v1.3-july-2017-redacted.pdf](#)