



Your reference:

Our reference: FOI_26_0399

E-mail: FOI

@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 19/08/2026

Dear

Gloucestershire Constabulary Freedom of Information request FOI_26_0399

On 27/04/2026 you sent an email constituting a request under the Freedom of Information Act asking the following:

1. Policies and governance

- (a) Copies of all policies, standard operating procedures, guidance documents, or directives — whether issued at force level or adopted from national guidance — that govern the use of generative AI tools by officers or staff, in force since 1 January 2023.
- (b) If no such policy or guidance exists, please confirm this.

2. Risk assessments and compliance

- (a) Copies of any Data Protection Impact Assessment (DPIA) completed in relation to the use of generative AI tools by officers or staff for any purpose, including administrative, investigative, or operational tasks.
- (b) If no DPIA has been completed for any generative AI tool, please confirm this.

3. Deployed tools and licensing

- (a) A list of any generative AI tools (including products bundled within existing software suites, such as Microsoft Copilot within Microsoft 365) that have been made available to officers or staff, and the date from which each tool was made available.
- (b) Whether access to any generative AI tool has been suspended or restricted since 1 January 2023, and if so, which tool, on what date, and any recorded reason for the suspension or restriction.

4. Training

- (a) Whether any training, e-learning, briefing, or written guidance on the use, limitations, or risks of generative AI tools has been provided to officers or staff, and if so, the date it was first made available.
- (b) Whether completion of such training is mandatory before officers or staff may use generative AI tools, or whether it is optional or advisory.

- (c) The number of officers and staff who have completed such training, if this figure is recorded, and the total number of officers and staff who currently have access to one or more generative AI tools.
- (d) If no training has been provided, please confirm this.

5. Incident recording and quality assurance

- (a) The number of occasions, if recorded, on which output from a generative AI tool used by officers or staff was subsequently identified as containing factual inaccuracies, fabricated information, or material errors — whether identified internally or by an external party — since 1 January 2023.
- (b) If no such records are held, please confirm this.

6. Audits and reviews

- (a) Copies of any audit, review, or evaluation — whether conducted internally or by an external body — of the force's use of generative AI tools.
- (b) If no audit or review has been conducted, please confirm this.

Gloucestershire Constabulary can confirm that it holds some relevant information relating to your request, however 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(1) – National Security
 Section 31(1) – Law Enforcement

Sections 24 and 31 are both qualified prejudice-based exemptions and it is therefore required to consider the harm in disclosure and conduct a public interest test.

Evidence of Harm

It is widely accepted that the disclosure of information through the FOI Act involves the release of information into the public domain and that criminals and hostile actors will monitor the responses to FOI requests in an attempt to gain information for nefarious purposes. This therefore must be considered in relation to the disclosure of information.

Previously the Force may have disclosed some of the requested information, however due to an ever-changing national threat profile facing law enforcement agencies, there is now an increased focus on artificial intelligence (AI) and the wider cyber security of the Force which in turn can affect the operational effectiveness of the Force, should the Force suffer a cyber-attack. Disclosing the requested information would leave the Force at a significantly increased risk of a cyber-attack as it would involve providing specific information surrounding the wider governance of AI within the Force alongside also providing exact technical information surrounding the Information Communication Technology (ICT) capabilities of the Force.

The disclosure of material relating to the Force's wider governance of AI such as policies, standard operating procedures, risk assessments and audit reports would reveal the extent of the Constabulary's current capabilities, limitations, safeguards and governance control measures. Disclosing such information would risk enabling those with criminal intent to further understand how AI technologies are used within the policing arena and identify perceived cyber vulnerabilities, weaknesses or gaps in the AI governance and compliance process.

The Constabulary has an overarching goal of enforcing the law, preventing, and detecting crime and protecting all the communities we serve through bringing offenders to justice. To achieve these objectives, the Constabulary relies on a range of digital technologies and information systems, including emerging technologies such as AI. Disclosure of information relating to the use and governance of AI would reveal intricacies of those systems and the compliance process which may place the overarching law enforcement goals at risk of being affected through disruption activities such as a cyber-attack.

If this FOI request was to be requested nationally, the disclosing of information could be used to understand cyber capabilities and governance on a national level as disclosure would also enable a geographical picture to be drawn up. For example, if each Police Force disclosed the requested information, this would contribute to a broader national picture regarding digital capabilities and governance within Policing. Which would contribute to a mosaic-like effect, whereby information would be obtained indicating each Police Force's digital capabilities and their governance strategy. This could significantly assist those seeking to target police systems.

Disclosing information could be detrimental to the public, as disclosing the information could assist a malicious actor by highlighting vulnerable forces and leaving those forces open to cyber-attacks and disruption.

Additionally, disclosing the information would also assist those seeking to circumvent police processes by providing insight into the controls, safeguards and mitigations in place relating to AI.

Public Interest Tests

Section 24 (1) National Security

Factors Favouring the Disclosure of Information

The police are accountable to the communities they serve. Disclosing the requested information would allow the public to be greater informed and contribute to any public debates surrounding the use and governance of AI within Policing. Disclosing the requested information would also increase public confidence and provide reassurance that there are stringent compliance frameworks in place covering AI within the Constabulary.

Factors Against the Disclosure of Information

The disclosure of the requested information would enable analysis of Constabulary wide cyber security risk management relating to AI and ICT security and infrastructure. This would provide in-depth knowledge to those seeking to conduct cyber-attacks or cyber disruption activities.

On a national level, if the requested information was disclosed, a national picture of capabilities, compliance, and governance would be able to be mapped. This would identify other Police Forces which may or may not have as stringent frameworks in place. This may place Gloucestershire Constabulary or another Force at risk of a cyber attack and/or cyber disruption activities through releasing the level of cyber security risk management relating to AI.

A cyber-attack or cyber disruption activities would significantly affect operational policing and be harmful to the public. Any such disclosure could be exploited by those seeking to cause harm, increasing the risk to the public. Therefore, any information that may lead to compromise of national security which ultimately affects law enforcement capabilities and

hinders the prevention and detection of crime, is not in the interest of the public to be disclosed.

Section 31 (1) Law Enforcement

Factors Favouring the Disclosure of Information

Disclosing the requested information would raise public awareness surrounding AI usage and governance within policing, this would allow the public to be more informed. Improved public awareness may lead to increased public confidence surrounding the topic area.

Factors Against the Disclosure of Information

Whilst there is public interest in providing reassurance that police forces are appropriately and effectively dealing with any threats, posed against technological capabilities, there is a strong public interest in safeguarding the welfare and safety of the public.

If Police cyber and ICT systems were successfully attacked, it could lead to the loss of confidentiality, integrity, and availability of police information. Any disclosure has the potential to undermine current and future technological integrity, which in turn compromises the overreaching goals which Police Forces are expected to carry out. Disclosing the requested information could risk jeopardising the daily running of police operations through the impact of any such cyber attack or disruption. Any such cyber-attack or disruption would significantly affect the administration of justice.

The public would not expect the Constabulary to disclose any such information which would place operational policing at risk and thus potentially place the public themselves at risk.

Balance Test

The Constabulary recognises the importance of transparency and accountability in relation to the adoption and use of emerging technologies such as AI.

Whilst there is a long-standing public interest in the transparency and accountability of policing and, it can be said that the topic area is of some public interest. There is, however, a substantial public interest in protecting information to ensure that operational policing can proceed unhindered to ensure that the service delivered to the public is not affected.

The security of not only the Constabulary but the country is of great importance, and the Constabulary would not seek to divulge any information if to do so would undermine overarching law enforcement goals or pose a risk to wider national security. Disclosure would increase the risk of harm to national security through the aggregation of information concerning the police technological infrastructure and the protective measures in place.

If Police cyber and ICT systems were successfully attacked, it could lead to the loss of confidentiality, integrity, and availability of police information. Any disclosure has the potential to undermine current and future technological integrity, which in turn compromises the overreaching goals which Police Forces are expected to carry out.

The public would not expect the Constabulary to disclose any such information which would place operational policing at risk and thus potentially place the public themselves at risk.

The points above highlight the merits for and against disclosure of the requested information. In every case, public safety is the paramount focus and the disclosure of any information which would place individuals and the Constabulary at risk or risk compromising the National Security of the United Kingdom, is not in the public interest. This would have a negative impact on law enforcement and national security.

Pursuant to Section 17(1) of the Act this letter acts as a refusal notice under the Freedom of Information Act 2000 in relation to your request.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - <https://ico.org.uk/>

Call their helpline - 0303 123 1113

Email - casework@ico.org.uk

Post – Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Disclosure Officer
Gloucestershire Constabulary