Gloucestershire Constabulary
Police Headquarters
No.1 Waterwells, Waterwells Drive
Quedgeley, Gloucester. GL2 2AN
www.gloucestershire.police.uk

Our reference: FOI_26_0956
E-mail: FOI@gloucestershire.police.uk
Direct dial: 01452 754304
Postal Address: As above
Date: 13/11/2026

Dear

Gloucestershire Constabulary Freedom of Information request FOI_26_0956

On 09/10/2026 you sent an email constituting a request under the Freedom of Information Act asking the following:

Under the Freedom of Information Act 2000, please provide the following recorded information held by the force.

Definition. In this request, 'AI tool' means any software that uses machine learning, a large language model, generative AI, predictive analytics or automated decision support. This includes AI features built into general products (for example Microsoft Copilot or ChatGPT) and data analytics platforms (for example Palantir). It covers tools in live use, in pilot, or used at any time since 1 January 2023.

Scope. I am not asking you to create new information, review individual cases or collate figures. I am asking for existing documents, registers and lists. Please exclude College of Policing guidance. I am not seeking operational detail about investigative or intelligence techniques, and any redaction can be applied at the narrowest level.

A. AI used internally in relation to officers and staff
For example workforce monitoring, integrity screening, vetting, professional standards, attendance, rostering, performance management or HR.
1. Whether the force uses, or has piloted since 1 January 2023, any AI tool for these purposes. If so, please state the product name, the supplier, the go-live date, and whether it is live or a pilot. Please also say whether the tool forms part of a national or regional framework or pilot.
2. The Data Protection Impact Assessment (DPIA) for each tool, including any updates or reviews.
3. The Equality Impact Assessment (EIA) for each tool. If none was completed, please confirm this in writing.
4. The terms of reference, or equivalent governance document, for any unit, board or group that oversees each tool.

We are committed to being an anti-discriminatory organisation. This means not only acting in a non-discriminatory way, but addressing systemic inequalities, disadvantage and discrimination.

5. Any internal policy, standard operating procedure or guidance on how outputs are used, how human review is applied, and how use of the tool is monitored and audited. Please include the most recent audit or review report, if one exists.
6. The contract value and the annual licence or running cost for each tool. A link to a published contract notice is acceptable.
7. Whether staff associations or trade unions were consulted before each tool was deployed, and any record of that consultation.

B. AI used by officers and staff in their work, internal and external facing
For example, generative AI assistants, transcription, summarisation, drafting, redaction, call triage and public-facing chatbots.
8. Any register or list of AI tools that have been authorised, procured or piloted. If no single list is held, a list of the titles of DPIAs that relate to AI tools will be sufficient.
9. The DPIA and the EIA for each tool listed at item 8.
10. Local policy or guidance on acceptable use of AI by officers and staff, including any rules on unapproved tools. Or confirm there is no guidance.
11. The training materials provided to officers and staff on the use of AI, or a description of their content. Please say whether the training is mandatory.
12. Guidance or policy on how AI use is logged, monitored and audited, and the most recent audit or review report. Or confirm that there is no guidance, policy or audit process.
13. The contract value and the annual licence or running cost for each tool listed at item 8.
14. The terms of reference for any AI board, ethics group or senior oversight forum, and the date it was established. Or confirm the board does not exist

C. General
15. Any consultation or correspondence with the Information Commissioner's Office about the tools above, including under UK GDPR Article 36.

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 to your request by virtue of the following exemptions:

Section 24(1) – National Security
Section 31(1) – Law Enforcement
Section 43(2) – Commercial Interests

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.

Section 43(2) exempts information whose disclosure would, or would be likely to, prejudice the commercial interests of any legal person (an individual, a company, the public authority itself or any other legal entity). This exemption is qualified and subject to the prejudice test and the public interest test.

Prejudice Test Considerations S.43(2) – Commercial Interests

The Constabulary can confirm that a prejudice test has been undertaken. Whilst the Constabulary is not at liberty to provide the prejudice test itself, the below serves as explanatory information surrounding the considerations and the test undertaken.

During the course of the prejudice test, the Constabulary must consider if disclosure of the requested information would, or would be likely to, prejudice our own commercial interests or the commercial interests of an engaged third party. Whilst not questioning or speculating on the motives of the requester, the disclosure of information via the Act, is considered to be a release into the wider public domain and whilst the Act places a presumption towards disclosing information where possible, considerations must also be given to releasing information into the public domain beyond the requester and any such associated risks of harm through disclosing the requested information.

It has been identified that the disclosure of information relating to the Constabulary's use, governance, and any contractual information including but not limited to individual products, costings, or specific licence arrangements surrounding the use of (AI) Artificial Intelligence would be likely to prejudice the commercial interests of both the Constabulary and any engaged suppliers.

Considerations must be given to the information being released in isolation and alongside information which is already present within the public domain. In relation to disclosing the requested information, it could provide competitors a valuable and significant insight into the current Constabulary arrangements for such products. Not only would disclosure of such information would be likely to prejudice the Constabulary's own commercial interests it would also risk prejudicing any engaged supplier's commercial interests where commercially sensitive material has been identified.

Additionally, it has been identified that current and future suppliers may note the disclosure of information and no longer seek to engage in the procurement process or supply their products to the Force owing to the knowledge that material identified as commercially sensitive could subsequently be disclosed into the public domain. There is a real and significant likelihood that disclosure would impact the Force and the supplier's ability to compete fairly within the marketplace and could adversely affect the Force's ability to secure best value for money from future contracts, which would not be in the publics interest as the Force is funded by the public purse.

It can be argued that disclosure of the requested information would risk affecting operational and commercial sensitivities.

Evidence of Harm – S.43(2) S.31(1) S.24(1)

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 when considering confirming or denying information held and in turn disclosing any such information.

Previously the Force may have disclosed some of the requested information, however due to an ever-changing national threat profile and emerging landscape facing law enforcement agencies alongside specific localised security assessments which have been undertaken. There is now an increased focus on cyber security and cyber resilience. As such, disclosing any information which may have the potential to aid criminals and hostile actors in evading detection, committing crime, and/or disrupting law enforcement functions would not be suitable to be released into the public domain and certainly not within the public interest.

The disclosure of specific named policing technologies which are or contain Artificial Intelligence (AI) would reveal the Constabulary's current capabilities and limitations whilst also risking 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 any technologies utilised for a policing purpose and/or functions which enable the effective running of the Constabulary. If this request was to be fielded on a national level, it would in turn provide an overview of each differing force's capabilities and any perceived limitations. This may result in individuals seeking to commit crime within the locality of perceived lesser capable police forces or seeking to commit cyber-attacks and disruptions on a national scale.

Providing the information sought within the request in the form of specific tools and named providers including cost alongside all associated governance and compliance documentation would not only pose the risk of prejudicing commercial interests of the Constabulary and engaged suppliers but also present a genuine cyber security risk to the Force, which in turn can affect the operational effectiveness of the Force, should the Force suffer a cyber-attack. Supplying the requested information would leave the Force at a significantly increased risk of a cyber-attack should hostile actors obtain the requested information and it would also provide a significant insight into tools and technologies which may or may not be used within the arenas of overt and covert policing as it would involve providing specific information surrounding the 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 which could be exploited.

Public Interest Test – S.43(2) S.31(1) S.24(1)

Factors Favouring Disclosure

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 alongside the reassurance that public funds are being spent accordingly.

Factors Favouring Non-Disclosure

The public entrust the Constabulary to protect the communities they serve, in relation to the Freedom of Information Act 2000 Act, this is evidenced through considering if disclosing information has the potential to disrupt law enforcement functions and poses a risk to core policing duties carried out in order to protect the community.

Measures are put in place to protect the communities we serve and to provide the information as requested would present the risk of individuals intent on disrupting law enforcement and/or targeting specific companies engaged in the AI law enforcement supply chain.

Considering the present security landscape and the increasing risk of cyber-attacks and cyber interference within the United Kingdom, no information which may aid criminality or increase risk should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duties of enforcing the law and serving the wider community through the detection of crime, the apprehension and prosecution of offenders, and the administration of justice.

The public entrust the Constabulary to make appropriate decisions with regard to their safety and protection when considering what information is placed into the public domain. To

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.

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 excepted to carryout. 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 Constabulary to carry out its core duties.

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 nor would the public expect the Constabulary to release any information which may lead to adverse commercial outcomes whereby the public purse is further strained.

Balance Test

The Police Service has the overarching goal of enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, services are utilised which are vital to core operational functions of the Force. Weakening these mechanisms would have a detrimental impact on law enforcement as a whole.

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 and significant 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 or detrimentally impacted.

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/or the Constabulary at risk.

To provide material as per your request increases the known risks of cyber-attacks and would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure.

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