

**Gloucestershire Constabulary**  
Police Headquarters  
No.1 Waterwells, Waterwells Drive  
Quedgeley, Gloucester. GL2 2AN  
[www.gloucestershire.police.uk](http://www.gloucestershire.police.uk)



Your reference:

Our reference: FOI\_26\_0038

E-mail: FOI

@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 21/05/2026

Dear

**Gloucestershire Constabulary Freedom of Information request FOI\_26\_0038**

On 09/01/2026 you sent an email constituting a request under the Freedom of Information Act asking the following:

please provide the following information for the period 1 January 2023 – 31 December 2024:

1. The number of occasions on which cyber or information security risks appeared on the agenda of your governing body (or equivalent oversight body).
2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight.
3. Whether documented criteria exist for escalating significant cyber incidents to the governing body or senior leadership (yes/no; if yes, please provide or summarise).
4. The number of governing body members (or equivalent) who completed cyber or information security training during this period, and the total number of members in that body.
5. Whether an independent assessment of your cyber security arrangements (e.g. internal audit, external review, or third-party assessment) was reported to the governing body during this period (yes/no; if yes, please state the type of assessment).

Under the Freedom of Information Act 2000 s1, I can confirm that Gloucestershire Constabulary holds some relevant information for part of your request

Please see the response to your request below.

1. The Constabulary has a robust process in place for management of risk and for those specific to cyber or information we have established specific forums in place that allow for the monitoring, escalation and reporting of necessary risks. There is an established Security Working Group (SWG) that has a standing agenda item around risk. This Group directly reports into the Information Governance Board (IGB).

In addition, we also have an established Senior Risk Information Officer forum with attendance from respective Information Security and information leads that meet regularly in order to discuss any associated risks appropriately.

2. The Information Governance Board.
3. Yes. However, we are unable to provide any further information as this is exempt by virtue of Section 31(1)(a)(b) Law Enforcement.
4. Cyber and Information security training is mandatory for all officers and staff.
5. Cyber security health checks are conducted by designated staff which have oversight of specific business areas and report upon a set basis. Alongside internal compliance and monitoring, the Constabulary is subject to health check monitoring by approved third parties.

### In relation to Q3

Section 17 of the Freedom of Information Act 2000 requires Gloucestershire Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states the fact, (b) specifies the exemption in question and (c) states (if not otherwise apparent) why the exemption applies.

In relation to the requested information, the following exemptions apply:

Gloucestershire Constabulary can confirm it holds information relevant to your request however as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

#### Section 31(3) - Law Enforcement

Section 31 is 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.

Disclosing the requested information would leave the Force at an increased risk of a cyber-attack due to sharing in-depth information around how we secure and defend our IT infrastructure. Releasing the requested information into the public domain, would highlight to the wider public the tools and techniques we as a Constabulary use to protect and monitor our IT infrastructure.

Releasing this information into the public domain would risk compromising our IT infrastructure and any such IT breach or service downtime resulting from the disclosure of information would prejudice the Force's ability to prevent and detect crime, the apprehension and prosecution of offenders.

## **Public Interest Test**

### **Factors in favour of disclosing information**

There is public debate and interest around how public funds are spent, disclosing the requested information would allow members of the public to be further informed around Constabulary spending. Providing information in respect of Gloucestershire Constabulary's ICT infrastructure would allow the public to be better informed on the performance of the network alongside maintaining public confidence through being open and transparent with the public around the use of public funds.

### **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 the Constabulary's ICT infrastructure.

There is a strong public interest in safeguarding the welfare and safety of the public. If 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 Law Enforcement, and could jeopardise the daily running of policing activity. The risk of affecting the function of the police service would be much greater.

### **Balance Test**

The security of the Constabulary is of great importance, and the Constabulary will not divulge any information if to do so would undermine overarching law enforcement goals or pose a risk to the effectiveness of operational policing.

Whilst there is a public interest in the transparency of policing and force IT infrastructure. There is also a very strong public interest in protecting information to ensure that core and key police operations are able to function in order to assist the communities we serve.

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater public awareness around the Constabulary network. Whilst there is always a public interest in the transparency of how a police force delivers an effective service there is an overwhelming public interest in ensuring that the force remains operationally effective and mitigates any potential risks to its core policing functions.

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 abilities.

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](mailto:casework@ico.org.uk)

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