

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



Your reference:

Our reference: FOI_26_0726

E-mail: FOI

@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 06/08/2026

Dear

Gloucestershire Constabulary Freedom of Information request FOI_26_0726

On 04/08/2026 you sent an email constituting a request under the Freedom of Information Act asking the following:

1) Total IT Expenditure:

Please provide the overall IT expenditure for each of the last three fiscal years.

2) Software Expenditure:

Please provide the total spend on software for each of the last three fiscal years. This should include initial software licence fees, software maintenance fees, and subscription fees but should exclude associated services such as installation.

3) Cell-Site, Communications Data and Digital Forensics Software – Supplier and Spend Detail:

For each of the last three fiscal years, please provide the following for any software used for cell-site analysis, communications data analysis (e.g. call data records / CDRs), digital device extraction analysis, or associated intelligence / link analysis. This includes, for example, products supplied by Forensic Analytics Ltd, Chorus Intelligence Ltd, or equivalent providers:

- the name of the supplier and the product(s) held;
- the total spend or annual contract value (including licence, maintenance and subscription fees, but excluding associated services such as installation, training or consultancy);
- the number of software licences or named users held;

Gloucestershire Constabulary can confirm that it holds some relevant information relating to your request, however the duty in s1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of the following exemptions.

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.

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.

In relation to your request, the following exemptions apply:

·Section 31(1) Law Enforcement

The exemption above is qualified and prejudice based therefore both a Harm Test and a Public Interest Test are required.

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 surrounding law enforcement processes and capabilities.

Previously the Force may have provided 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 what ICT systems as a Force we or do not use. Disclosing the requested information would leave the Force at an increased risk of a cyber-attack due to disclosing the spend relating to specific Information Communications Technology (ICT) areas within the Constabulary.

Releasing information which highlighted areas of increased spending or areas which had a distinct difference or perceived lack of funding when compared over a 3-year period could be used to gauge any perceived weaknesses within the ICT capabilities of the Constabulary. Additionally, the same would apply to any specific spending surrounding software. Disclosing information which identifies individual suppliers of software would risk impacting on operational policing, due to releasing information which would enable individuals to take actions to prevent the detection of crime if they were fully aware of all of the software used by the Constabulary.

The Constabulary has an overarching goal of enforcing the law, preventing, and detecting crime and protecting all of the communities we serve. To achieve these objectives, all forces utilise Information Technology essential to front line services. Disclosure of the Constabulary's ICT infrastructure, including financial spend information surrounding the use of specific software applications and capabilities, or the lack thereof, would reveal intricacies of those systems, thereby highlight vulnerabilities and compromise individual force information assurance. Disclosure would also enable a geographical picture to be drawn up by those individuals who are intent on 'hacking' police systems; some of these individuals may include terrorists or terrorist organisations.

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 disruption of Information Technology systems; thus, compromising the effective delivery of operational law enforcement which in turn, is met by an increase of criminal offending.

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 systems and software would allow the public to be better informed on the performance of the systems 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 police force Technology capabilities, there is a strong public interest in safeguarding the welfare and safety of the public.

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.

If information ICT systems were successfully attacked, it could lead to the loss of confidentiality, integrity, and availability of police information which would in turn affect operational policing.

Balance Test

The security of not only the Constabulary but the country is of great importance, and the Constabulary will not divulge any information if to do so would undermine overarching law enforcement effectiveness or pose a risk to wider national security.

Whilst there is a public interest in the transparency of policing and force ICT systems, 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. Alongside this, there is also the ongoing aim of ensuring that the National Security of the United Kingdom is maintained

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 and/or national security.

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