

Chief Constable
Chief Constable Robert Carden
Police Headquarters
Carleton Hall Penrith,
Cumbria
CA10 2AU



27th November 2024

Dear

FREEDOM OF INFORMATION REQUEST – FOI 989/24 – ICT Infrastructure

I refer to your request for information which was received by Cumbria Constabulary on 4th November 2024. I note you seek access to the following information:

1. *What is your annual IT Budget for 2024, 2025 & 2026?*

2. *Storage:*

- A) *What storage vendor(s) and models do you currently use?*
- B) *What is the capacity of the storage data in TB & How much of this is utilised?*
- C) *What were the installation dates of the above storage vendor(s) and when do you estimate you will refresh them? (Month/Year)*
- D) *Do you have any extended warranties, if so, with which supplier?*
- E) *Which reseller(s) provides the above technology, what was the value of the contract, and when does the contract(s) end?*

3. *Server/Compute:*

- A) *What number of physical servers do you have?*
- B) *What server vendor(s) and models do you currently use?*
- C) *What were the installation dates of the above server vendor(s) and when do you estimate you'll refresh them? (Month/Year)*
- D) *Do you have any extended warranties, if so, with which supplier?*
- E) *Which operating systems are used?*
- F) *Are you currently using VMWare, do you have any plan to move away from VMWare?*
- G) *Which reseller(s) provides the above technology, what was the value of the contract, and when does the contract(s) end?*

4. *End User Technologies*

- A) *How many users within your organisation receive a laptop or desktop device?*
- B) *What laptop and desktop device vendor(s) and models do you currently use?*
- C) *How many mobile phones are used within your organisation?*
- D) *What mobile vendor(s) do you currently use?*
- E) *Which reseller(s) provides the above technology and when does the contract(s) end?*
- F) *Have you transitioned to Windows 11, or do you have a plan in place to transition to Windows 11.*
- G) *Is your current device estate compatible with Windows 11?*
- H) *What deployment methods are you using (e.g SCCM or Intune/Autopilot)?*

5. *Managed Print Services*

- A) *What number of MFDs and production print devices do you have?*



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



- B) Who is the current vendor(s) and the suppliers(s) and when do these contracts end?
C) What is your annual spend on Managed Print Services?
D) Do you use any document management or scanning / storage services? If so please can you provide the details of the supplier and the end date of the contract.

6. ITSM/ESM & Business Process Automation

- A) What IT Service Management / Enterprise Service Management tool do you currently use and who supplies it?
B) When was your current system installed and when does the contract or support expire?
C) Do you utilise Business Process Automation or have a plan to implement this tooling?

7. Do you have a managed/shared service with any other organisations?

8. Do you normally purchase equipment and services as a capital investment (CapEx) or ongoing operational charges (OpEx)?

Your request for information has now been considered and I can confirm Cumbria Constabulary does hold information you request, however I will be citing the exemption Section 31 (1) to questions which relate to storage, installation dates, vendors, contract dates, service management tools and warranties.

Section 31 (1) (a)(b), Law Enforcement.

Please Note: Previously, we would disclose this information, however, there has since been a key change in the stance taken, which is outlined in the exemption below. In this case, we consider that disclosure of the information would be likely to make the police service more open to malicious attacks on our computer systems. The risk of cyber-attacks, with the threat more likely since the war in Ukraine, therefore, posing an increased risk more recently.

Section 31(1)(a) exempts information if its disclosure would or would be likely to prejudice the prevention and detection of crime.

As a qualified and prejudice-based exemption, I am required to evidence the harm and apply the public interest test.

Evidence of Harm

Every effort should be made to release information under Freedom of Information. However, a FOIA response is considered to be a release to the world, as once the information is published, the public authority has no control over what use is made of that information.

The Police Service is charged with enforcing the law, preventing, and detecting crime and protecting 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 on-going plans for specific software applications and capabilities, or the lack thereof, would reveal intricacies of those systems, thereby highlighting vulnerabilities and compromising 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. In terms of duty of care, this would be detrimental to the public, as disclosure 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.



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



Public Interest Test

Factors favouring disclosure – Disclosing the specific details of certain ICT infrastructure, would allow the public to be better informed on the health state and performance of each forces Information Technology platform. In addition, forces are required to demonstrate efficient services to local taxpayers and satisfy audit requirements. This would provide transparency regarding the use of public funds in so much as highlighting that funds are being used correctly and appropriately, to ensure all Data Centres have adequate software, which results in the smooth running of force Technology systems.

Factors favouring non-disclosure - 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. 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. In addition, by revealing ICT software, this is intelligence to those who would wish to exploit vulnerabilities in the service. This may lead to the compromise of force IT systems which ultimately affects law enforcement capabilities and hinders the prevention and detection of crime or terrorism.

Balance Test

The security of the country is of paramount importance and the Police service will not divulge any information, if to do so would undermine law enforcement and therefore compromise the work of the police service. Whilst there is a public interest in the transparency of policing and force infrastructure, including the Police ICT infrastructure, there is a very strong public interest in safeguarding the integrity of these systems in place.

The points above highlight the merits for and against disclosure of the requested information. Disclosure would undoubtedly provide a greater openness and transparency to the community at large regarding the Information Technology resources available to the police, and whilst there is always a public interest in the transparency of how a police force delivers effective law enforcement, there is a very strong public interest in safeguarding the intricacies and tactical capabilities of the software used when dealing with information.

I am aware of the immense importance for Public Authorities to demonstrate a level of openness and transparency, I am of the opinion that protecting the tactical capability of Cumbria Constabulary must take precedence in this case. With this in mind, it is my decision that the balance of the public interest lies in the non-disclosure of the exempted information.

I can provide information in relation to questions 1, 3a, 4a, 4c, 5a, 5c and 8 which have been provided from the Constabulary's Finance, ICT and Commercial departments.

Question 1

The Constabulary work on financial years for budgeting and are as follows:

23/24 £6,436,341

24/25 £7,490,741

25/26 No information held, as the budget has not yet been approved.

Question 3

a/ Cumbria Constabulary have 52 physical servers

Question 4



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD

Proudly supporting those who serve.



- a/ 2166 users within the organisation have the use of a laptop or desktop device
- c/ 1283 mobile phones are used within the Constabulary

Question 5

- a/ Cumbria Constabulary have 61 MFDs and production print devices
- c/ Annual spend is £4000 (excludes £29000 click charges)

Question 8

Purchases are dependant on the actual requirement but mainly will be ongoing operational charges.

Whilst every care has been taken in the retrieval of the information provided, please do not hesitate to contact us for clarification, if you do have any issues or queries relating to this data.

Complaint Rights

Your attention is drawn to the attached sheet, which details your right of complaint.
I would like to take this opportunity to thank you for your interest in Cumbria Constabulary.



EMPLOYER RECOGNITION SCHEME

BRONZE AWARD
Proudly supporting those who serve.

