

OFFICIAL



Heddlu Police

DYFED-POWYS

FOI Reference: 421/2021

Request:

1. Do you have a cloud strategy? (Please provide a link to the strategy)
 - A) Yes
 - B) No
2. When was the cloud strategy defined?
3. If yes, what is the focus of your cloud strategy?
 - A) All in on public cloud (no private cloud or on-premise infrastructure)
 - B) Cloud First (new services in public cloud with some on premises infrastructure or private cloud)
 - C) Hybrid cloud (some combination of one or more public clouds, private cloud and on-premises)
 - D) Private cloud (no public cloud)
4. What public cloud(s) do you use?
 - A) AWS
 - B) Alibaba Cloud
 - C) Azure
 - D) Google Cloud Platform
 - E) Oracle Cloud
 - F) UK Cloud
5. What percentage of your applications and/or workloads is on premise?
 - A) 0%
 - B) 10% - 25%
 - C) 25% - 50%
 - D) 50% - 75%
 - E) 100%
6. What percentage of your applications and/or workloads is in the public cloud?
 - A) 0%
 - B) 10% - 25%
 - C) 25% - 50%
 - D) 50% - 75%
 - E) 100%
7. What percentage of your data is on premise?
 - A) 0%
 - B) 10% - 25%
 - C) 25% - 50%

- D) 50% - 75%
 - E) 100%
8. What percentage of your data is in the public cloud?
- A) 0%
 - B) 10% - 25%
 - C) 25% - 50%
 - D) 50% - 75%
 - E) 100%
9. What percentage of your infrastructure is legacy?
- A) 0%
 - B) 10% - 25%
 - C) 25% - 50%
 - D) 50% - 75%
 - E) 100%
10. Do you have third-party services or solutions on premise that are not cloud-ready or fit for cloud migration?
- A) Yes
 - B) No
11. What workloads or functions have you moved to the cloud? (Multiple answers. Please specify other if not listed)
- A) Office productivity (e.g. Microsoft 365, Google Workspace)
 - B) Citizen-facing digital services (e.g. GOV.UK)
 - C) Back-office applications (e.g. transaction processing)
 - D) Artificial Intelligence, Machine Learning, cognitive services
 - E) Software development/DevOps
 - F) Corporate functions (e.g. HR, Finance, CRM)
 - G) Intranet
 - H) Public website
 - I) Backup, business continuity and disaster recovery
 - J) Other
12. What challenges did you face when moving to the public cloud? (Multiple answers. Please specify other if not listed)
- A) Migrating certain applications
 - B) Legacy infrastructure
 - C) Different refresh cycles
 - D) Difficulty proving cost illustrations
 - E) Funding paths (Capex/Opex)
 - F) Data gravity
 - G) Data Classification
 - H) Licensing concerns
 - I) Data privacy concerns
 - J) Offshoring & data residency
 - K) Lack of in-house skills
 - L) Vendor lock-in/ Egress cost prohibitive
 - M) Other
13. What percentage of your infrastructure do you plan to be public cloud based in 12 months' time?
- F) 0%
 - G) 10% - 25%

- H) 25% - 50%
- I) 50% - 75%
- J) 100%

14. What percentage of your infrastructure do you plan to be public cloud based in three years' time?
- A) 0%
 - B) 10% - 25%
 - C) 25% - 50%
 - D) 50% - 75%
 - E) 100%
15. How much has your organisation spent on public cloud since the Government's G-Cloud or 'cloud-first' policy was introduced in 2012?
16. How much has your organisation spent on on-premise infrastructure since the Government's G-Cloud or 'cloud-first' policy was introduced in 2012?
17. How much has your organisation spent on cloud/infrastructure consultancy services in FY 20-21?
18. How much was spent on public cloud data egress charges in FY 20-21?

Clarification sought:

With regards to your Q16 - How much has your organisation spent on premise infrastructure since the Government's G-Cloud or 'cloud-first' policy was introduced in 2012?

Are you asking for server and storage costs specifically or server, storage, networking, firewall etc.?

There will always be a requirement for on premise infrastructure for networking and firewalls, therefore we are not sure if they should be excluded.

Response received from applicant:

With reference to question 16, please include server, storage, networking, firewall etc. too.

Responses:

I can confirm that Dyfed-Powys Police does hold the information requested, the details of which are as follows:

- 1) No - No specific strategy, however in our ICT Strategy we do refer to Cloud first.
- 2) Not applicable, which is based on the response provided in relation to question 1.
- 3) Cloud First.
- 4) Azure.
- 5) No information held as percentage figures are not recorded.
- 6) No information held as percentage figures are not recorded.

- 7) No information held as percentage figures are not recorded.
- 8) No information held as percentage figures are not recorded.
- 9) No information held as percentage figures are not recorded.
- 10) Yes.
- 11) Office productivity – Partial.
Public website
Other – Digital Evidence Management

Additionally, Dyfed-Powys Police can neither confirm nor deny that it holds any other information with regard to an exempt body 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 24(2) – National Security**
- **Section 31(3) – Law Enforcement**

Sections 24 and 31 are prejudice based qualified exemptions and both evidence of harm and public interest considerations need to be articulated to the applicant.

Harm in confirming or denying information is held

Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. By revealing whether any other information is held in relation to cloud based data and applications that are extraction technology, will in itself be revealing tactical information which would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders.

Factors favouring confirming or denial – S31

Confirming or denying that Dyfed Powys police force holds further information would raise the general public's awareness around the full extent of policing capabilities and show responsibility to delivery of effective operational law enforcement.

Factors against confirming or denying – S31

By confirming or denying whether further information is held could compromise Dyfed Powys police forces law enforcement capabilities and the effectiveness of the force will be reduced. To confirm or deny if further information is held could undermine current and/or future strategies when carrying out investigations and gathering evidence may be compromised.

The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, confirming or denying if any further information is held would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases.

Factors favouring confirming or denial – S24

Confirming or denying that any other information exists relevant to the request would lead to a better informed public and the public are entitled to know how public funds are spent. The information simply relates to national security and disclosure would not actually harm it.

Factors against confirming or denial - S24

To confirm or deny whether Dyfed Powys police force hold any other information would allow inferences to be made about the nature and extent of national security related activities which may or may not take place. This could enable terrorist groups to take steps to avoid detection, and as such, confirmation or denial would be damaging to national security.

By confirming or denying any policing arrangements of this nature would render national security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure on the UK and increase the risk of harm to the public.

Balancing Test

As always the Freedom of Information Act has a presumption of disclosure, unless when balancing the competing public interest factors the prejudice to the community outweighs the benefits. In this case, there is an argument for confirming or denying, inasmuch as the public have a right to know how forces deliver effective operational law enforcement, and that every effort is made to gather all relevant evidence, including where cloud based data and applications that are extraction technology are used. But this must be balanced against the negative impact these disclosures can make.

Law Enforcement is reliant on community engagement, intelligence and evidence gathering and when it is appropriate, information is given to the public. What has been established in this case is the fact that confirming or denying that any further information relating to technologies is used would be harmful and have an adverse effect on the investigative process and on the public prevention or detection of crime and the apprehension or prosecution of offenders. This places the victims of such offending at a greater risk towards their health and wellbeing and is not an action the Police Service would be willing to take. These negatives outweigh any tangible community benefit and therefore the balance does not favour disclosure at this time.

12) Funding paths.

13) No specific target

14) No specific target

15) 2.2 million

16) No information held

17) Zero (£0)

18) Zero (£0)

It should be noted that owing to the systems adopted by Dyfed-Powys Police in relation to the recording of such matters the information provided may or may not be accurate.

This Force's response to your questions should not be used for comparison purposes with any other response you may receive.

(This is a response under the Freedom of Information Act 2000 and disclosed on 06/07/21)