



Our Ref: 002754/20

Your Ref:

Address Correspondence to: Information Management

Date 01 September 2020

### **Freedom of Information Act 2000**

I write further to your request for information received 19/08/2020.

I note you seek access to the following information:

1. How does your police force currently access and manage its data and applications?

- On premises
- In a public cloud
- In a private cloud
- Hybrid cloud model
- Other, please state:

2. What approximate percentage of your data and applications are currently 'in the cloud'?

- Zero
- 1-25%
- 26-50%
- 51-75%
- 76-99%
- All of our applications and data are hosted in the cloud

3. Is your police force considering investing in cloud infrastructure and technologies - such as software, platform or infrastructure as a service (SaaS, PaaS or IaaS) - in the next 12 months?

- Yes
- No
- Don't know

4. Is your IT department outsourcing or downsizing its physical IT infrastructure, e.g. on premise servers and physical hardware, in favour of a cloud model?

- Yes – we have already done so
- Yes – we are planning to do so in the next 12 months
- Yes – we are in the process of doing so
- No – we do not plan to do this

5. Are all of your police officers that work with IT / computers able to access data files and applications when working remotely / out in the field?

- Yes
- No
- Don't know

6. How much has your police force spent on outsourcing IT in the last five years? This refers to budget spent on devices used by third parties/contractors/outsourced employees as well as outsourcing itself  
?

Year    Total amount spent on outsourcing IT, incl. outsourcing IT services and procuring devices for third parties    Specific amount spent only on procuring devices for third parties/contractors/outsourced employees

2019

2018

2017

2016

2015

7. Does your police force report back on information technology use related greenhouse gas emissions?

- Yes – and we have specific targets to meet
- Yes – but we don't have specific targets to meet
- No
- Don't know

If your police force does have 2020 targets on information technology use related greenhouse gas emissions, please answer:

8. Are you on track to meet your 2020 targets for information technology use related greenhouse gas emissions?

- Yes – we're on track to exceed that target
- Yes – we're on track to meet that target
- No
- Don't know

Following receipt of your request, searches were conducted within Leicestershire Police to locate information relevant to your request.

**Your request for information has now been considered and the information asked for is as follows: -**

1. How does your police force currently access and manage its data and applications?

- On premises
- In a public cloud
- In a private cloud
- Hybrid cloud model
- Other, please state:

**Mix of on-prem, private cloud and third party cloud-hosted services**

2. What approximate percentage of your data and applications are currently 'in the cloud'?

- **1-25%**

3. Is your police force considering investing in cloud infrastructure and technologies - such as software, platform or infrastructure as a service (SaaS, PaaS or IaaS) - in the next 12 months?

- **Yes**

4. Is your IT department outsourcing or downsizing its physical IT infrastructure, e.g. on premise servers and physical hardware, in favour of a cloud model?

**None - We will be reviewing our cloud strategy which will help inform our future direction**

5. Are all of your police officers that work with IT / computers able to access data files and applications when working remotely / out in the field?

- Yes

6. How much has your police force spent on outsourcing IT in the last five years? This refers to budget spent on devices used by third parties/contractors/outsourced employees as well as outsourcing itself

**Leicestershire Police do not have true out-sourced services but third-party service contracts -Quatrix & CDW contracts, and laptop for the CDW engineer**

**Quatrix = £250k**

**CDW = £115k**

**For the CDW engineer, there is also a laptop at £1200**

7. Does your police force report back on information technology use related greenhouse gas emissions?

If your police force does have 2020 targets on information technology use related greenhouse gas emissions, please answer:

8. Are you on track to meet your 2020 targets for information technology use related greenhouse gas emissions?

Please see the link to our current Police Crime Plan

<https://www.leics.pcc.police.uk/DOCUMENT-LIBRARY/Planning-and-Money/Police-and-Crime-Plan/2017-2021/Police-and-Crime-Plan-2017-2021.pdf>

With reference to information as to whether or not Leicestershire Police uses Cloud based extraction technology we can neither confirm nor deny by virtue of **s24(2) National Security, and s31(3) Law Enforcement**

Harm in confirming 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. In this case the information relates to the extraction of data from individuals' mobile devices, albeit victim or offender. By revealing whether information is held in relation to the specific 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 XXX force holds information would raise the general public's awareness around techniques used to extract information from mobile phones and show responsibility to delivery of effective operational law enforcement.

Factors against confirming or denying – s31

By confirming or denying whether information is held could compromise XXX forces law enforcement capabilities and the effectiveness of the force will be reduced. To confirm or deny if 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 the information is held in relation to gathering evidence from mobile phones, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

#### 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 Leicestershire Police force hold any 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 that every effort is made to gather all relevant evidence, including extracting data from mobile phones, 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 information relating to technologies used when extracting data 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.

Leicestershire Police provides you the right to ask for a re-examination of your request under its review procedure. Letters should be addressed to Information Manager, Corporate Services Department at the above address. If you decide to request such a review and having followed the Force's full process you are still

dissatisfied, then you have the right to direct your comments to the Information Commissioner who will give it consideration.

Yours sincerely

Freedom of Information Officer

Leicestershire Police

Leicestershire Police in complying with their statutory duty under sections 1 and 11 of the Freedom of Information Act 2000 to release the enclosed information will not breach the Copyright, Designs and Patents Act 1988. However, the rights of the copyright owner of the enclosed information will continue to be protected by law.

Applications for the copyright owner's written permission to reproduce any part of the attached information should be addressed to The Information Manager, Leicestershire Police Headquarters, St. Johns, Enderby, Leicester LE19 2BX.