



Our Ref: 002095/21

Your Ref:

Address Correspondence to: Information Management

Date 22 July 2021

Freedom of Information Act 2000

I write further to your request for information received 21/06/2021.

I note you seek access to the following information:

1. *Are your digital forensic labs ISO 17025 certified?*
2. *Has your force ever used a third-party organisation/service to carry out digital forensics? If so:*
 - a. *Which third-party organisation/service did you use?*
 - b. *On how many separate occasions have you used them during the period 2019-2021?*
 - c. *What safeguards are in place to ensure third-party services are certified?*
3. *Does your digital forensic lab follow MOPI guidelines?*
 - a. *If not. Can you provide the guidelines followed by your force?*
4. *Where is your digital evidence stored? (Internally/ Externally)*

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. Are your digital forensic labs ISO 17025 certified? **Yes**
2. Has your force ever used a third-party organisation/service to carry out digital forensics? If so:
 - a. Which third-party organisation/service did you use?
 - b. On how many separate occasions have you used them during the period 2019-2021?
 - c. What safeguards are in place to ensure third-party services are certified?

Leicestershire Police do not routinely use third parties to carry out digital forensic examinations for digital devices such as phones and computers. The question is however quite broad as "digital forensics" is a wide reaching phrase. We have in the past for example used forensic video companies to complete image assessment for major enquiries and to complete activities such as vehicle identification that we are not qualified to do. Where we use such services they are classed as expert witnesses and as such their duty is to the court to provide information that is fair, unbiased and assists the court in understanding. Their qualifications to do this can, and do, come under scrutiny in a court. Leicestershire Police do not keep a central record of these "out source" requests and they will usually come from individual departments to registered experts. The company would be approved by the a Senior personnel and all the relevant checks would be completed."

The information captured at Q2a and Q2b will be exempt by virtue of section 31(1)(a)(b) Law Enforcement.

The Harm Test process requires Leicestershire Police to consider any possible harm that may arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- Leicestershire Police and the wider policing service
- Other bodies

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

<https://www.app.college.police.uk/app-content/information-management/>

Commercial Forensic Service Providers are vitally important in the Criminal Justice system - not only do they play a crucial role by supporting UK Policing with backlogs in the Digital Forensics arena, but they provide Defence teams with access to independent forensic experts to support their clients.

Whilst not in any way questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any forensic service providers used by Leicestershire Police would be extremely useful to those involved in criminality as it would enable them to create a map of those most used by police Forces. Forensic Service Providers can be targeted by malicious actors, for example in 2019 Eurofins (one of the UKs largest FSPs) suffered a highly sophisticated ransomware attack which severely disrupted UK Policing and the Criminal Justice system.

<https://www.helpnetsecurity.com/2019/06/24/eurofins-ransomware-attack/>
<https://www.theguardian.com/science/2019/jul/05/eurofins-ransomware-attack-hacked-forensic-provider-pays-ransom>

By providing a list of forensic service providers, Force by Force, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those providing the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Factors favouring Disclosure - Confirming the names of Forensic Service Providers would be of interest to the public, namely give insight into the forensic processes used to solve crimes.

Factors favouring Non-Disclosure - Measures are put in place to protect the community we serve and as evidenced within the harm, to provide a detailed list of Forensic Service Providers would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

Taking into account the current security climate within the United Kingdom, and the recent Eurofins cyber-attack, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

Balance Test - The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, external services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. To provide the names of the FSPs despite the known risks of cyber-attacks would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure of the FSP used for digital forensics.

3. Does your digital forensic lab follow MOPI guidelines?

Yes

a. If not. Can you provide the guidelines followed by your force?

4. Where is your digital evidence stored? (Internally/ Externally)

Internally

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.