



**LEGAL SERVICES
BOARD**

Legal Services Board
The Rookery
2 Dyott Street
London WC1A 1DE

www.legalservicesboard.org.uk

14 September 2021

FoI request reference: 20210831-01

Thank you for your request for information about ransomware and IT systems.

The LSB does hold the information that you have requested, please find this set out below:

1. In the past three years has your organisation:
 - a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)- **None**
 - i. If yes, how many?
 - b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.) **No**
 - c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.) **No**
 - d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
No
 - i. If yes was the decryption successful, with all files recovered?
 - e. Used a free decryption key or tool (e.g. from <https://www.nomoreransom.org/>)? **No**
 - i. If yes was the decryption successful, with all files recovered?
 - f. Had a formal policy on ransomware payment? **No**
 - i. If yes please provide, or link, to all versions relevant to the 3 year period.
 - g. Held meetings where policy on paying ransomware was discussed? **No**
 - h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
 - i. If yes at what cost in each year? **No**
 - i. Used existing support contracts for malware, ransomware, or system intrusion investigation? **Yes**
 - j. Requested central government support for malware, ransomware, or system intrusion investigation? **No**
 - k. Paid for data recovery services? **Yes for routine data back ups**
 - i. If yes at what cost in each year? **Cannot isolate this cost as it forms part of the contract cost.**
 - l. Used existing contracts for data recovery services? **Yes because of restore from backups.**
 - m. Replaced IT infrastructure such as servers that have been compromised by malware? **No**
 - i. If yes at what cost in each year
 - n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? **No**
 - i. If yes at what cost in each year?

- o. Lost data due to portable electronic devices being mislaid, lost or destroyed? **No**
 - i. If yes how many incidents in each year?
- 2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? **Yes**
 - a. If yes is this system's data independently backed up, separately from that platform's own tools?
A cloud based solution is used and the data is independently backed up using a separate backup tool
- 3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)
 - a. Mobile devices such as phones and tablet computers
No
 - b. Desktop and laptop computers
No
 - c. Virtual desktops
N/A
 - d. Servers on premises
Yes
 - e. Co-located or hosted servers
N/A
 - f. Cloud hosted servers
Yes
 - g. Virtual machines
Yes
 - h. Data in SaaS applications
Yes
 - i. ERP / finance system
Yes
 - j. We do not use any offsite back-up systems
N/A
- 4. Are the services in question 3 backed up by a single system or are multiple systems used?
Multiple systems are in use
- 5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?
Yes (Microsoft 365). Already migrated in 2019 so cloud migration costs have been committed in prior years and so no existing budget.
 - a. How many Software as a Services (SaaS) applications are in place within your organisation? **5**
 - b. How many have been adopted since January 2020?
Software as a service since Jan 2020 – Zoom, Vuelio (CRM software)

We note that in accordance with the LSB's publication scheme under FOIA, we routinely publish FOIA responses with personal data redacted.

If you are dissatisfied with this response to your request for information, you have the right to ask for an internal review / to submit a complaint within 40 working days of this response (see [LSB's Freedom of information – Complaints procedure](#)).

If you are dissatisfied with the outcome of your complaint, you may refer the matter to the Information Commissioner for a decision. Please be aware that the Commissioner will be unlikely to make a decision until you have been through our internal complaints procedure first. You can contact the Commissioner through their website: <https://ico.org.uk/>.

The reference for your request, which should be quoted in all correspondence, is: 20210831-01.