Dear

Freedom of Information Response (Our Ref: K/21/426)

Thank you for your Freedom of Information (FOI) request dated 31 August 2021, reference K/21/426.

Your request read:

“I am writing to you under the Freedom of Information Act 2000 to request the following information from University of Leeds. Please can you answer the following questions:
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?)
   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.)
   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.)
   d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
      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/)?
      i. If yes was the decryption successful, with all files recovered?
   f. Had a formal policy on ransomware payment?
      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?
   h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
      i. If yes at what cost in each year?
      i. Used existing support contracts for malware, ransomware, or system intrusion investigation?
   j. Requested central government support for malware, ransomware, or system intrusion investigation?
   k. Paid for data recovery services?
      i. If yes at what cost in each year?
   l. Used existing contracts for data recovery services?
   m. Replaced IT infrastructure such as servers that have been compromised by malware?
      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?
i. If yes at what cost in each year?
o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
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?
a. If yes is this system’s data independently backed up, separately from that platform’s own tools?

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 
b. Desktop and laptop computers 
c. Virtual desktops 
d. Servers on premise 
e. Co-located or hosted servers 
f. Cloud hosted servers 
g. Virtual machines 
h. Data in SaaS applications 
i. ERP / finance system 
j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used?

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

6. How many Software as a Services (SaaS) applications are in place within your organisation?
a. How many have been adopted since January 2020?”

The University of Leeds holds some of this information.

For your convenience we have responded to each of your questions in turn 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?)
      i. If yes, how many?

Like other Higher Education institutions, the University of Leeds is under continuous ransomware attacks. We are withholding the number of incidents under section 31(1)(a) of the FOI Act.
To release the number of attempted attacks over the last three years provide those who have attempted to attack the University with information which could be used to establish whether their attempt(s) was recognised by the University. This information could be used by the responsible party or parties to adapt future attacks, prioritising methods and/or elements which do not appear to have been detected while discontinuing efforts which are readily noticed. This would make us more vulnerable to future attacks, which jeopardises our ability to provide services to students, alumni and staff. The information is therefore exempt under section 31(1)(a).

We appreciate that there is a strong public interest in understanding how organisations such as the University of Leeds responds to cyber-attacks. However, we consider that there is a very strong public interest in ensuring we do not increase our own vulnerability to attacks in future. We therefore conclude that the overwhelming public interest in this case is in favour withholding the requested information.

b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

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.)

d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
   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/)?
   i. If yes was the decryption successful, with all files recovered?

We address these questions together. There have been no such incidents.

f. Had a formal policy on ransomware payment?
   i. If yes please provide, or link, to all versions relevant to the 3 year period.

We do not have a written policy on ransomware payments. However, the University’s default position is to adopt the advice from the National Cyber Security Centre and JISC and not pay ransoms.

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?

No

j. Requested central government support for malware, ransomware, or system intrusion investigation?

No

k. Paid for data recovery services?
   i. If yes at what cost in each year?

No

l. Used existing contracts for data recovery services?

No

m. Replaced IT infrastructure such as servers that have been compromised by malware?
   i. If yes at what cost in each year?

No

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
   i. If yes at what cost in each year?

No

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
   i. If yes how many incidents in each year?

None

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?

No

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
b. Desktop and laptop computers  
c. Virtual desktops  
d. Servers on premise  
e. Co-located or hosted servers  
f. Cloud hosted servers  
g. Virtual machines  
h. Data in SaaS applications  
i. ERP / finance system  
j.

Yes for servers on premise; co-located or hosted servers; cloud hosted servers; virtual machines; ERP/finance systems, and some data in SaaS applications (varies by vendor).

4. Are the services in question 3 backed up by a single system or are multiple systems used?

Multiple

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

There is a strategy but the budget for this is part of a wider programme.

6. How many Software as a Services (SaaS) applications are in place within your organisation?

We do not hold a complete list of all SaaS solutions being used by every part of the University. However, we can advise that the main SaaS applications are: M365, ServiceNow, Minerva, Sonic Foundry, Service Now, and StREAM.

a. How many have been adopted since January 2020?

One

We hope this information is helpful. If you have any questions about this email, however, please do not hesitate to contact us on foi@leeds.ac.uk

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request a review of our decision, you can request an Internal Review. Requests for Internal Review should be made in writing using the following contact information:

Post: Mr D Wardle  
Deputy Secretary  
The University of Leeds  
Leeds  
LS2 9JT

Email: foi@leeds.ac.uk
Requests for Internal Review should be submitted within 40 working days of receiving the University’s response to your request. Further information about how the University manages Freedom of Information requests and about our complaints procedure is also available on our website (www.leeds.ac.uk).

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review/complaints procedure provided by the University. The Information Commissioner can be contacted at: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Sincerely

Chloe Wilkins
Freedom of Information Officer
University of Leeds