London Borough of Barnet,
2 Bristol Avenue, Colindale,
London NW9 4EW
1 September 2021
Our ref: 7615248

Thank you for your request received on 1 September 2021, for the following information:

I am writing to you under the Freedom of Information Act 2000 to request the following information from London Borough of Barnet. 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

We have processed this request under the Freedom of Information Act 2000.

Response

We believe that the exemptions detailed below apply to all the information you requested and so we are withholding that information. Please see the Refusal Notice below.

I am writing to you under the Freedom of Information Act 2000 to request the following information from London Borough of Barnet. 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

We believe that the exemptions detailed below apply to all the information you requested and so we are withholding that information.

Please see the Refusal Notice below.

This information is exempt from disclosure under Section 31(3) of the Freedom of Information Act 2000. Section 31 of the FOIA relates to Law Enforcement, and Section 31(3) removes the public authority's duty to confirm or deny whether information is held if to do so would or would be likely to prejudice law enforcement.

It is the council's view that the confirmation or denial of the possession of information relating to the council's cyber resilience, would be likely to compromise the council's information security strategies by giving cyber criminals insight into vulnerabilities which may, or may not, exist.

Although the bona fides of the requester may be genuine FOI responses are public information and are made to the world. Section 31(3) is a qualified exemption, as such we have gone on to perform a public interest test in order to assess the public interest arguments for and against declaring whether or not the requested information is held.

In applying this exemption, we have had to balance the public interest in withholding the information against the interest in favour of disclosure.

Factors in favour of disclosure

- Confirmation of possession would demonstrate a commitment to transparency with regard to the council's undertakings, and could provide assurance that the council have robust IT infrastructure in place.

Factors in favour of withholding

- Maintaining the integrity and security of the council's systems
- Preventing cyber-attacks and similar against the council systems.
- Revealing whether or not the information requested is held or applicable to the London Borough of Barnet would be likely to offer cyber criminals insight into not only the strengths of the council's cyber security ,but also any potential weaknesses that may exist. This could ultimately result in a future cyber attack. One of the reasons that cyber security measures are in place is to protect the integrity of personal and sensitive personal information.
- It is clear to see how the occurrence of a future cyber-attack would prejudice the council's legal duty to safeguard personal information from loss, theft, inappropriate access or destruction, which is why Section 31 has been employed in this case.
- A cyber attack could have catastrophic consequences for council services for residents exacerbated by the dependence on these services at a time of a national emergency from Covid-19.

On balance the public interest in maintaining the exemption outweighs that in confirming or denying whether information is held and therefore the council neither confirms nor denies whether this information is held. In all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

Further information

If you are interested in the data that the council holds you may wish to visit Open Barnet, the council's data portal. This brings together all our published datasets and other information of interest on one searchable database for anyone, anywhere to access. http://open.barnet.gov.uk/

Advice and Assistance : Direct Marketing

If you are a company that intends to use the names and contact details of council officers (or other officers) provided in this response for direct marketing, you need to be registered with the Information Commissioner to process personal data for this purpose. You must also check that the individual (whom you wish to contact for direct marketing purposes) is not registered with one of the Preference Services to prevent Direct Marketing. If they are you must adhere to this preference.

You must also ensure you comply with the Privacy Electronic and Communications Regulations (PECR). For more information follow this Link www.ico.org.uk

For the avoidance of doubt the provision of council (and other) officer names and contact details under FOI does not give consent to receive direct marketing via any media and expressly does not constitute a 'soft opt-in' under PECR.

Your rights

If you are unhappy with the way your request for information has been handled, you can request a review within the next 40 working days by writing to the Information Management Team at: foi@barnet.gov.uk. Or by post to Information Management Team (FOI) London Borough of Barnet, 2 Bristol Avenue, Colindale, NW9 4EW

If, having exhausted our review procedure, you remain dissatisfied with the handling of your request or complaint, you will have a right to appeal to the Information Commissioner at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (telephone: 0303 123 1113; website www.ico.org.uk). There is no charge for making an appeal.