London Borough of Barnet,
2 Bristol Avenue,
Colindale,
London NW9 4EW

7

7 April 2021
Our ref: 7090952

Thank you for your request received on 5 March 2021, for the following information:

I would like to submit an FOI request regarding the challenges your council has faced during the pandemic.

Specifically, I would like responses to the following questions:

Question

1)

a) How many people do you employ?

b) How many of your employees were moved to remote working from March 2020?

2)

a) Did COVID-19 and the move to remote working mean you had to make additional investments in security in order to support remote working?

b) If yes, how much (if possible)?

3)

a) (If answered YES to question 2 (a) above) Where did the budget for additional investments in security in order to support remote working come from?

a. From the wider IT budget

b. From reducing investment in other services

c. From council savings

d. From selling council assets - e.g. property.

4) Does your organisation plan to continue using remote working more post-

COVID-19 than it did pre-COVID-19?

a. Yes

b. No

5) For each of the following, can you indicate whether you a) have invested more in the item below after March 2020, and b) plan to invest further in the future.

a. Secure VPN access for remote workers

b. Encryption for remote workers (e.g. software encryption, thumb drives)

c. Identity and access management

d. Security Information and Event Management (SIEM) tools (e.g. Splunk)

e. Endpoint security

f. Increased security training for remote workers

g. Security posture assessment to understand any impacts from the move to remote working and identify any gaps in security

ANSWER OPTIONS:

a. We have invested more

b. We plan to invest further in the future

6) Have any of your employees been prevented from working remotely because it wasn't possible to guarantee secure access to data?

a. Yes

b. No

7)

a) Have you had reported to you and/or identified any cyber-attacks made against remote employees (e.g., phishing, man-in-the-middle attacks, brute force attacks against VPNs)?

a. How many of these were identified / reported from March 2020 onwards?

b. How many were identified / reported in the 12 months before March 2020 (i.e. March 2019 - February 2020)?

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

Response

I can confirm that London Borough of Barnetholds the information you requested.

However, we consider that the following exemptions apply to some of the information requested. The remaining information is not withheld and is below.

1)

a) How many people do you employ?

1465 employees

b) How many of your employees were moved to remote working from March 2020?

All staff that have the ability to work remotely have been supported in doing so.

2)

a) Did COVID-19 and the move to remote working mean you had to make additional investments in security in order to support remote working?

b) If yes, how much (if possible)?

3)

a) (If answered YES to question 2 (a) above) Where did the budget for additional investments in security in order to support remote working come from?

a. From the wider IT budget

b. From reducing investment in other services

c. From council savings

d. From selling council assets - e.g. property.

IT is provided by Capita under a 10 year outsource contract which started in 2013. You can find out more information about the contract on the following page of our website
https://open.barnet.gov.uk/dataset/customer-and-support-group-csg-contract

The information requested is exempt under the refusal notice available at the above link.

4) Does your organisation plan to continue using remote working more post-COVID-19 than it did pre-COVID-19?

a. Yes

b. No

The council has for several years pre-covid, had the ability for officers to work both flexibly and remotely. This will not change in so far as the ability to work in this manner will continue, the council is currently considering how this will look longer term and any decisions will be taken in line with government guidance.

5) For each of the following, can you indicate whether you a) have invested more in the item below after March 2020, and b) plan to invest further in the future.

a. Secure VPN access for remote workers

b. Encryption for remote workers (e.g. software encryption, thumb drives)

c. Identity and access management

d. Security Information and Event Management (SIEM) tools (e.g. Splunk)

e. Endpoint security

f. Increased security training for remote workers

g. Security posture assessment to understand any impacts from the move to remote working and identify any gaps in security

ANSWER OPTIONS:

a. We have invested more

b. We plan to invest further in the future

This was provided by our outsourced provider as part of the contract.

6) Have any of your employees been prevented from working remotely because it wasn't possible to guarantee secure access to data?

a. Yes

b. No

No

7)

a) Have you had reported to you and/or identified any cyber-attacks made against remote employees (e.g., phishing, man-in-the-middle attacks, brute force attacks against VPNs)?

a. How many of these were identified / reported from March 2020 onwards?

b. How many were identified / reported in the 12 months before March 2020 (i.e. March 2019 - February 2020)?

See Refusal Notice below

Section 31 Law Enforcement

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.

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.

For 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

Against Disclosure:

• 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 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 cyberattack.

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, nappropriate access or destruction, which is why Section 31 has been employed in this case.

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.

I believe that your service area may hold some of the information requested.

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.