17 April 2018
Our ref: 4198100

Thank you for your request received on 8 February 2018, for the following information:

I am writing as a research volunteer at the Open Rights Group. We are conducting a study to better understand filtering and blocking of websites on the public estate, to understand what content and sites are inaccessible and why. I am writing to ask about this in relation to libraries under local authority control. Please answer all questions in relation to the libraries that you are responsible for.

We would like to know, in relation to your publicly accessible Internet networks, or Internet networks for your clients:

1. The categories of content blocked or filtered, eg:
a) Security or Malware.
b) Content types, eg adult, alcohol etc.
c) Statistics relating to the requests blocked or filtered, eg how many site requests are filtered or blocked per category.

2. Monitoring requirements you have for users, eg if you record or may record their Internet usage.

3. The supplier of your blocking or filtering software.
a) Eg, Sophos, Forcepoint, Palo Alto etc.

If these policies operate on a per library basis, or are a decision not taken by the council, please provide a contact email for the managers of each library in your jurisdiction so we can make enquiries on a more granular basis.

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

Response

The council holds the information requested and it is attached/ the answers to your questions are below

We would like to know, in relation to your publicly accessible Internet networks, or Internet networks for your clients:

1. The categories of content blocked or filtered, eg:

a) Security or Malware.

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 equested 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, inappropriate 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.

b) Content types, eg adult, alcohol etc.

See attached list of content types from the Barnet 'Corporate' browsing policy from the corporate console, which is similar to that used by the library service.

c) Statistics relating to the requests blocked or filtered, eg how many site requests are filtered or blocked per category.

I have attached a list of blocked categories from the Barnet 'Corporate' browsing policy from the corporate console, which is similar to that used by the library service.

2. Monitoring requirements you have for users, eg if you record or may record their Internet usage.

The library PC booking system retains details of library card number, name and address of the user, date of birth, PC used and times used.

3. The supplier of your blocking or filtering software.
a) Eg, Sophos, Forcepoint, Palo Alto etc.

Forcepoint.

If these policies operate on a per library basis, or are a decision not taken by the council, please provide a contact email for the managers of each library in your jurisdiction so we can make enquiries on a more granular basis.

These are based on ForcePoint recommended settings that have been reviewed by the Council Library service, and is a general Library management decision, Hannah Richens, Library Manager email xxxxxx.xxxxxxx@xxxxxx.xxx.xx

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: xxx@xxxxxx.xxx.xx.Or by post to Information Management Team (FOI) The London Borough of Barnet, North London Business Park, Oakleigh Road South, London, N11 1NP

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.