Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 9 June 2022

Public Authority: London Borough of Hackney
Address: Information Management Team
1 Reading Lane
London
E8 1DQ

Decision (including any steps ordered)

1. The complainant has requested information from London Borough of Hackney ("the Council") in relation to its cyber security arrangements. The Council refused to disclose the requested information, citing sections 31(1)(a) and 31(1)(g) by virtue of 31(2)(i) as a basis for non-disclosure.

2. The Commissioner's decision is that the Council has correctly applied section 31(1)(a). As the Commissioner considers that this applies to all of the requested information, he has not gone on to consider the Council's application of section 31(1)(g) by virtue of section 31(2)(i).

3. The Commissioner requires no steps to be taken.

Request and response

4. On 16 December 2020, the complainant wrote to the Council and requested information in the following terms:

"What reviews if any have taken place on cyber security measures for Hackney Council over the last 2 years? Please detail the number of reviews, their format and any recommendations from these reviews.

- Did Hackney Council provide any additional training on cyber security for employees who were working from home due to the Covid-19 pandemic?

- Please detail what training was provided and whether it was completed by all staff working from home.

- What training has been provided to Hackney Council staff over the past 2 years to raise awareness and help prevent cyber-attacks?"

5. The Council responded on 26 January 2021. It refused to disclose the requested information, citing section 31(1)(a) of FOIA (prevention or detection of crime) as a basis for non-disclosure.

6. On 21 February and 4 May 2021 the complainant wrote to the Council seeking an internal review stating that he accepted the application of section 31(1)(a) in relation to the first two parts of his request, however he did not consider that it applied to the third and fourth parts.

7. Following the Commissioner's intervention via an Information Notice served on the Council on 15 November 2021, the Council eventually, on 15 February 2022, provided the complainant with an internal review response. The reviewer upheld the original decision regarding section 31(1)(a) and also sought to apply section 31(1)(g) by virtue of section 31(2)(i) of FOIA.

Scope of the case

8. The complainant first contacted the Commissioner on 9 June 2021 to complain about the way their request for information had been handled.

9. The Commissioner has considered the Council's handling of the complainant's request, in particular its application of section 31(1)(a) to the third and fourth parts of the complainant's request.

Reasons for decision

10. Section 31(1) of FOIA states that: "Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice-

    (a) the prevention or detection of crime

11. Section 31 is a prejudice based exemption and is subject to the public interest test. This means that not only does the information have to prejudice one of the purposes listed, but also that it can only be withheld if the public interest in the maintenance of the exemption outweighs the public interest in disclosure.

12. In order for section 31 to be engaged, the following criteria must be met:

- the actual harm which the public authority claims would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption (in this case, the prevention or detection of crime);
- the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and,
- it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.

The Council's view

13. The Council has cited the 2013 case of Yiannis Voyias v Information Commissioner and the London Borough of Camden[1], which states that information not explicitly held for the purposes of preventing or detecting crime can be exempt from disclosure if found to be prejudicial, as long as the risk of harm has been appropriately detailed.

14. The Council is of the belief that the requested information (ie. specific details of the Council's cyber security arrangements) could be combined with other information (potentially already in the public domain) to cause harm, an effect known as the 'mosaic effect.'

15. The Council states that any information disclosed by it is based upon a risk assessment. For any release of information, the Council has to consider the potential to put the rights and freedoms of data subjects at risk by publishing information concerning Hackney's information security practices that could potentially be used to cause harm. This includes, but is not limited to, employee training and access to the Council's network for remote working.

16. The Council has not specified which threshold of prejudice it is relying upon – 'would' or 'would be likely to.' However, its use of the terminology 'potential' and 'could' leads the Commissioner to consider

[1] [2013] UKFTT EA_2011_0007 (GRC)

whether the lower threshold of prejudice, i.e. 'would be likely to' is applicable.

Is the exemption engaged?

17. The Commissioner recognises, in his published guidance[2], that section 31(1)(a) will cover all aspects of the prevention and detection of crime. He accepts that the exemption can be used to withhold information that could make anyone more vulnerable to crime. The Council's argument in this case is that disclosure could put the Council at higher risk of a cyber-attack.

18. In light of the subject matter of the request in this case, the Commissioner is satisfied that the prejudice envisaged by the Council is relevant to the particular interests that those limbs of the exemption are designed to protect.

19. The Commissioner is also satisfied that the Council has demonstrated a causal relationship between the disclosure of the information at issue and the prejudice that sections 31(1)(a) is designed to protect.

20. With respect to the likelihood of prejudice, the Commissioner's guidance states[3] "If an authority claims that prejudice would occur they need to establish that either:

- the chain of events is so convincing that prejudice is clearly more likely than not to arise. This could be the case even if prejudice would occur on only one occasion or affect one person or situation; or

- given the potential for prejudice to arise in certain circumstances, and the frequency with which such circumstances arise (ie the number of people, cases or situations in which the prejudice would occur) the likelihood of prejudice is more probable than not".

21. Having duly considered the arguments put forward by the Council regarding disclosure of information relating to its cyber security arrangements having the potential to increase the risk of cyber-crime

[2] https://ico.org.uk/media/for/organisations/documents/1207/law-enforcement-foi-section-31.pdf

[3] https://ico.org.uk/media/for/organisations/documents/1214/the_prejudice_test.pdf

against the Council, the Commissioner's view is that the Council has demonstrated sufficiently that prejudice 'would be likely to' be caused by disclosure.

22. He therefore finds the exemption engaged in relation to the information withheld by virtue of section 31(1)(a).

The public interest test

23. Section 31 is a qualified exemption, which means that the authority must also consider the public interest arguments in favour of both disclosure and maintaining the exemption.

Public interest arguments in favour of disclosure

24. The Council recognises that there is an inherent public interest in transparency and accountability in relation to the procedures and decision making of public authorities. This would be particularly true of security arrangements.

25. The complainant's argument is that it is in the public interest to know whether the Council fulfilled its duty in providing training to employees who would be working from home and accessing the Council's networks remotely. In his view this was an obvious threat that a local authority should be shown to be doing all they can to mitigate.

Public interest arguments in favour of maintaining the exemption

26. In this case, the requested information is not in the public domain and is, in the Council's view sensitive and significant. The Council has also taken account of the wider context of significant and growing cyber threats which continue to present a substantial risk (as highlighted in the recent NCSC advisory notice of 9 February 2022)[4].

27. The Council further states that the need for transparency and accountability is addressed by the independent investigation which is currently being carried out in respect of previous cyber-attacks.

Balance of public interest factors

28. The Commissioner will always accord significant weight to the public interest in transparency and accountability regarding the decision-

[4] https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware.

making processes and procedures of public authorities, especially in respect of things like security arrangements, as any weakness in these could potentially greatly affect the public.

29. However, the Commissioner has taken into account the Council's arguments that disclosure of the information would potentially increase the risk of cyber-crime.

30. The Commissioner accepts that any information, disclosure of which increases the potential for crime against the public authority should not be released lightly. He considers that there would have to be highly strong and significant countervailing public interest factors in favour of disclosure, in order to outweigh the public interest in prevention or detection of crime.

31. As there is clear evidence of previous cyber-attacks against the Council, which are currently being investigated, the Commissioner considers that this investigation will address issues of openness and transparency in relation to cyber security arrangements. Disclosure of the withheld information could potentially increase the risk of further cyber-attacks, which the Commissioner fully accepts should be prevented in any way possible.

32. Therefore the Commissioner considers that the public interest arguments in favour of maintaining the exemption, when balanced against those in favour of disclosure, significantly outweigh the latter in all the circumstances of the case.

Other matters

33. The Commissioner issued an Information Notice to the Council as detailed in paragraph above. This was not complied with for several months due to apparently being sent to an e-mail address that was no longer in use by the Council.

34. The Commissioner has updated his contact details for the Council, to prevent future re-occurrences of this. The Commissioner would also expect the Council to ensure the re-direction of inactive e-mail accounts to the correct address in future. In respect of the initial delay in carrying out an internal review, the Commissioner fully understands and accepts the difficulties experienced by public authorities during the Covid-19 pandemic. Nevertheless, he would like to take this opportunity to remind the Council of its responsibilities in carrying out an internal review within the recommendations and guidelines set out by the Commissioner in his guidance and relevant Code of Practice.

Right of appeal

35. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

36. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

37. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Deirdre Collins
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF