Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**25 October 2023**
Public Authority:	**Redcar & Cleveland Borough Council**
Address:	**Redcar and Cleveland House** **Kirkleatham Street** **Redcar** **Cleveland** **TS10 1RT**

Decision (including any steps ordered)

1. The complainant requested from Redcar & Cleveland Borough Council ("the council") final project documentation for information for ICT projects completed in 2022. The council initially applied section 43(2), however it subsequently amended its position to apply section 31(1)(a) (prevention and detection of crime).

2. The Commissioner's decision is that the council was correct to apply section 31(1)(a) to withhold the information from disclosure.

3. The Commissioner does not require further steps.

Request and response

4. On 21 June 2023, the complainant wrote to the council and requested information in the following terms:

> "*I am creating an Artificial Intelligence chat assistant for Project Managers who work in Local Government. I request, under the Freedom of Information Act, the following information:*
>
> *Final project documentation for all ICT projects completed during 2022 including:*
>
> ** Project Plan (Project Initiation Documentation)*
> ** Risk Register*
> ** Issue Register*
>
> *I would like you to provide this information in the following format:*
>
> *As CSV files, spreadsheets, text or Word documents*."

5. The council responded on 26 June 2023. It refused to provide the information, citing section 43(2) of FOIA (prejudice to commercial interests).

6. Following an internal review, the council wrote to the complainant on 27 June 2023. It upheld its initial decision.

Scope of the case

7. The complainant contacted the Commissioner on 26 July 2023 to complain about the way their request for information had been handled. Their complaint is that the council had wrongly withheld the information from disclosure. They acknowledged that some information may need to be redacted from the information which falls within the scope of their request, however they argue that some information could be disclosed with sensitive information redacted from disclosure.

8. During the course of the Commissioner's investigation, the council withdrew its reliance upon section 43(2). It amended its position to apply section 31(1)(a) to withhold the information from disclosure.

9. This decision notice therefore analyses whether the council was correct to apply section 31(1)(a) to withhold the information from disclosure.

Reasons for decision

10. Section 31(1)(a) of FOIA says that:

> *"Information …. is exempt information if its disclosure under this Act would, or would be likely to, prejudice-*
>
> *(a) the prevention or detection of crime,"*

11. The council highlighted that the withheld information, particularly that held within its IT risk and issue registers, contains information on vulnerabilities within its systems, which, if exposed to criminals, could help them launch successful cyber-attacks against the council's systems.

12. The council's clarified that its IT project plans detail the systems and underlying infrastructure that it has and will be implementing. It argued that a disclosure of such detailed information would enable any potential attacker to focus their efforts on any known or zero-day vulnerabilities when attempting to access its systems and data as this will become plain from reading the documents. Additionally, it argued that the council is sometimes reliant on 3rd parties (suppliers) to resolve IT security issues. It considered that revealing the withheld information could also put others at risk that use these systems.

13. Given the widespread nature of cyber-attacks, the council argued that a disclosure of the information would be likely to prejudice the prevention and detection of crime. It noted that it is constantly under attack from cyber criminals including the probing of firewalls, phishing emails etc. It argued that placing detailed information around its IT systems and existing vulnerabilities into the public domain would considerably increase the chances of a successful attack and therefore prejudice the prevention or detection of crime.

14. It said that it also considered that government advice advises against enabling possible attackers to passively obtain information about a network which would put them in a better position to identify vulnerabilities and utilise attacks, increasing their chances of success and lowering the chance of them being detected.

The Commissioner's analysis

15. The Commissioner accepts that the potential prejudice described by the council clearly relates to the interests which the exemption contained at section 31(1)(a) FOIA is designed to protect; the prevention and detection of crime.

16. The Commissioner's guidance on section 31 states that:

> *"For example, section 31(1)(a) – prevention or detection of crime, can protect information on a public authority's systems which would make it more vulnerable to crime."*[1]

17. The Commissioner is also satisfied that the prejudice being claimed is "real, actual or of substance", and that there is a causal link between disclosure and the prejudice claimed. It is clearly logical to argue that the disclosure of detailed information about its systems and software and the risks and issues it has identified within that could be used to identify any security systems weaknesses. This could, in turn be used to successfully target its IT systems for criminal purposes. Withholding the information from disclosure therefore serves to protect the council's IT structure from cyber-attacks.

18. Disclosures under FOIA are considered to be to the whole world. Given the scale and consistency of cyber-attacks, the Commissioner accepts that the prejudice which the council has foreseen would be likely to occur if the information were to be disclosed to the whole world. The information requested by the complainant provides oversight of the projects being implemented, and the risks and issues which arise as a result of this. Information of this nature will clearly include information which, if disclosed, would raise the likelihood of successful cyberattacks being targeted against the council's systems.

19. Finally, the council responded to the complainant's suggestion that some of the information could be provided with any sensitive information redacted. It argued that this wasn't possible as, for ICT projects, the very fact that a project is working in a particular area or with a particular supplier would be sufficient information to cause a severe risk.

20. The Commissioner is persuaded by this argument. Identifying the types of software in use can allow cyber-criminals to narrow down and identify known vulnerabilities within that specific software, and from there, they can attempt to exploit these within the council's system to see if they are exposed and vulnerable. Additionally, given the technical complexities of software and hardware systems, it may be difficult to establish which sections within the withheld information provide information which would make it more vulnerable to attacks.

---

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

21. The Commissioner is therefore satisfied that section 31(1)(a) was correctly engaged by the council.

22. Section 31(1)(a) is a qualified exemption. Therefore, the Commissioner must consider whether, in all the circumstances of the case, the public interest in maintaining the exemption at section 31(1)(a) outweighs the public interest in disclosing the information.

23. The test is whether, in all the circumstances of the case, the public interest in the exemption being maintained outweighs that in the information being disclosed. If it does, then the information can be withheld under the exemption.

Public interest test

24. The council recognised that there is a public interest in creating greater transparency regarding which IT systems it uses, how it operates and the systems upon which it spends public funds. The Commissioner agrees that disclosure would help to increase openness and transparency in relation to the IT projects and systems purchased and used by the council. It would also highlight to interested parties whether the security measures which have been implemented are appropriate and proportionate to the risks which the system faces.

25. However, the council argues that there is a greater public interest in protecting its ability to prevent information on any vulnerabilities within its IT systems being published, and thereby increasing the likelihood of its systems being successfully attacked.

26. The Commissioner accepts that cyber-crime is a growing issue. Disclosing information which could be used to identify any IT vulnerabilities within the council's systems would put its IT infrastructure at serious risk.

27. A disclosure which makes its systems more vulnerable to a successful attack raises the risk of its the information held on its systems being exposed, stolen or encrypted via ransomware. The council highlighted that if it was successfully hacked or its systems were damaged it would have to expend significant resources, time and money to recover from such an attack. There is also the risk of the council receiving fines if the personal data it holds is exposed. Details held on local council's systems will include personal data of members of the public and council employees, including sensitive personal data.

28. Whilst the Commissioner notes that the risk of a successful attack may be relatively small, due to the antivirus, firewall and other security systems which the council will have in place, the Commissioner notes that the implications of such an attack puts the council's systems, its ability to carry out its functions, and personal data at risk. There is therefore a very strong public interest in protecting such an attack from occurring, including taking measures to prevent information which might heighten the risk of a successful attack being made from being disclosed.

29. The Commissioner has a duty to consider the broader public interest and he acknowledges that there is a very significant public interest in protecting society from crime, and from the impacts of crime; criminal acts affect public safety, wellbeing, and the public purse. Disclosing details of IT systems employed by the council would allow cyber-criminals a greater opportunity to identify vulnerabilities within the council's IT systems, thereby increasing the likelihood of successful attacks being made against its systems.

30. Whilst the Commissioner recognises a general public interest in the disclosure of the requested information, he considers that there is a much stronger public interest in protecting detailed information about its systems from disclosure in order ensure that cyber-attacks against it are not made easier and more likely to be targeted successfully.

31. The Commissioner has therefore decided that there is a stronger public interest in avoiding any prejudice to the ability to prevent and detect crime. As such the Commissioner's conclusion is that the public interest in maintaining the exemption in section 31(1)(a) of FOIA outweighs the public interest in disclosure.

32. The Commissioner's decision is therefore that the council was correct to apply section 31(1)(a) to withhold the information from disclosure.

Right of appeal

33. 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: 0203 936 8963
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

34. 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.

35. 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 .....

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