Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 28 November 2024

Public Authority: Denbighshire County Council
Address: Council Offices
County Hall
Wynnstay Road
Ruthin
Denbighshire
LL15 1YN

Decision (including any steps ordered)

1. The complainant requested details of the Case Management system used by the Children's Social Care department for Denbighshire County Council (the Council). The Council refused the information citing 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 2 July 2024, the complainant wrote to the Council and requested the following information:

> "What case management system does Children's Social Care use? i.e. Liquid Logic/LCS."

5. The Council responded on 3 July 2024. It refused the request, citing section 31(1)(a) of FOIA on the basis that disclosure would leave it more vulnerable to cyber-attacks.

6. Following an internal review, the Council wrote to the complainant on 11 July 2024, upholding its original decision.

Scope of the case

7. The complainant contacted the Commissioner on 11 July 2024 to complain about the way their request for information had been handled. They disagreed with the Council's decision to refuse the request under the exemptions cited.

8. The scope of the Commissioner's investigation is therefore to consider whether the council was correct to apply section 31(1)(a) to withhold the information from disclosure.

Reasons for decision

9. 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,"

10. 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]

11. The complainant does not accept that the exemption is engaged. As supporting evidence, they included five hyperlinks to identical requests to other public authorities for the same, or similar information. Without exception, each public authority provided the requested information.

12. The Council however considers that the disclosure of the requested information, would be likely to put it at risk of being targeted by cyber criminals as it would reveal the specific IT systems/software used and would allow cyber criminals to target any specific vulnerabilities to gain unlawful access to information. It added that Cybercrime is now

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

widespread and systems are under daily attack from phishing and probing firewalls.

13. The Council confirmed that it uses appropriate technical or organisational measures to prevent sensitive personal data being deliberately compromised including a cyber resilience plan which protects known vulnerabilities, zero-day attacks on new vulnerabilities, or misconfigured software, or systems shared between hackers on the dark web. It added that withholding software names provides extra protection for the security of personal data.

14. The Council quoted from the Commissioner's decision notice IC-247621-J0C9[2] in respect of Redcar and Cleveland Borough Council which referred to Government advice against enabling possible attackers to passively obtain information about a network. It stated that:

> "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."

15. The Council further stated that it is rare to know how a cyber-attack comes about, or what information criminals have relied upon. However, it quoted the National Cyber Security Centre comments that:

> "Exploitation of known vulnerabilities in software remains the greatest cause of security incidents."

16. Whilst each case is considered on its own merits, the Commissioner asked the council to consider why other public authorities were able to disclose similar information, but it considered that the information should be exempt from disclosure. The Council said that the other requests were dated between 2021 and June 2023. It said that these decisions would not therefore take account of recent cybercrime or the current information security landscape.

The Commissioner's analysis

17. The Commissioner would point out that disclosures under the FOIA are considered to be to the world at large.

18. Given the scale and consistency of cyber-attacks, the Commissioner is satisfied that the prejudice being claimed is "real, actual, or of

[2] https://ico.org.uk/media/action-weve-taken/decision-notices/2023/4027227/ic-247621-j0c9.pdf

substance", and that there is a causal link between disclosure and the prejudice claimed.

19. In reaching this decision, the Commissioner is mindful that identifying the types of software in use can allow cyber-criminals to narrow down and identify known vulnerabilities within the specific software, and from there, they can attempt to exploit these within the Council's system to see if they are exposed and vulnerable.

20. It is therefore logical to argue that the disclosure of the name of a particular case management system would increase the risks to the authority that cyber criminals would successfully attempt to target their systems.

21. Further, the Commissioner considers that the risk of cyber criminals hacking a system which holds sensitive personal information in respect of children's social care, could cause significant harm.

22. The Commissioner therefore accepts that the potential prejudice described by the Council clearly relates to the interests which the exemption contained at section 31(1)(a) of the FOIA is designed to protect; the prevention and detection of crime. On this basis, the Commissioner is satisfied that section 31(1)(a) was correctly engaged by the Council.

23. 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. If it does, then the information can be withheld under the exemption.

Public interest test

24. The Council has acknowledged that there is a general public interest in disclosure of information held by public authorities as it facilitates openness and transparency.

25. The Council also accepts that disclosure would encourage public participation in its decision making and could increase public confidence in its software systems.

26. The Council has also acknowledged that disclosure of the requested information would allow public scrutiny of its decisions and its expenditure of public money in respect of its case management system for children's social care.

27.

28. However, the Council argues that there is a greater public interest in protecting its software systems from attack by cyber-criminals.

29. It considers that Ransomware organisations could encrypt its information, blocking support for the residents of Denbighshire. It has added that it could potentially affect millions of items held by the Council, and argued that it is obliged to protect the public purse from damaging interference with its IT systems. Ransomware would be a particularly costly result of disclosure in terms of time and money to recover from such an attack.

30. The Council has further argued that there is a public interest in protecting the personal data held on its IT systems against unauthorised and unlawful processing. It has added, that in this case, the data held on the case management system in question is particularly sensitive as it involves the processing of children's personal data, including social work records and court records.

31. The Council also considers that cybercrime would harm its reputation, and that it would lose the confidence of its residents in its ability to protect its systems and software from being compromised.

The Commissioner's conclusion

32. The Commissioner has considered the arguments for and against the disclosure of the requested information put forward by the Council. He accepts that there is a general public interest in transparency and accountability about decision making and the expenditure of public money.

33. However, whilst the risk of a successful attack may be relatively small due to antivirus systems, firewalls and other systems 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 (sensitive) personal data at risk. There is therefore a very strong public interest in protecting information from disclosure which might heighten the risk of a successful attack from being disclosed.

34. 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.

35. Disclosing the name of the software system it uses for children's social care would allow cyber-criminals a greater opportunity to identify whether it is using a system with known vulnerabilities, and to better identify any potential vulnerabilities within its systems. This would increase the likelihood of successful attacks being made against it.

36. Although the risks highlighted may be relatively small, they are nevertheless genuine risks, and the effect of a successful attack on its systems would be great and would have a significant and harmful effect on the vulnerable individuals it has on its database.

37. The Commissioner has therefore decided that the public interest in avoiding any prejudice to the ability to prevent and detect crime clearly outweighs the limited value in the disclosure of the requested information in this case.

38. As such, the Commissioner's conclusion is that the public interest in maintaining the exemption in section 31(1)(a) of the FOIA, outweighs the public interest in disclosure.

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

Right of appeal

40. 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

41. 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.

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

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