pennsylvania
OFFICE OF OPEN RECORDS

FINAL DETERMINATION

IN THE MATTER OF	:	
	:	
TODD SHEPHERD,	:	
Requester	:	
	:	
v.	:	**Docket No: AP 2026-3659**
	:	
OWEN J ROBERTS SCHOOL DISTRICT,	:	
Respondent	:	

On July 15, 2026, Todd Shepherd ("Requester") filed a request ("Request") with the Owen J Roberts School District ("District") pursuant to the Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101 *et seq*., seeking, *inter alia*:[1]

> [1.] All reports, summaries, dashboards, or analyses generated by the [D]istrict's internet content filtering system (including but not limited to GoGuardian / Securly / Lightspeed) showing website or domain access that was permitted or unblocked on [D]istrict-issued devices for the period January 1, 2024 through the date of this [R]equest.
>
> [2.] All records showing permitted or unblocked access to YouTube.com, including any video-level URL data, on district-issued [D]evices for the same period.
>
> [3.] All network traffic logs, firewall logs, or web access logs maintained by the [D]istrict's IT department showing domains or URLs successfully accessed on [D]istrict-issued devices for the same period.

On August 24, 2026, after invoking a thirty-day extension to respond, *see* 65 P.S. § 67.902(b), the District denied the portion of the Request quoted above, arguing that the disclosure

[1] The Request contained five other Items that the District granted in part and are not at issue on appeal.

of responsive records would be reasonably likely to threaten the safety or security of an information storage system or jeopardize computer security. *See* 65 P.S. §§ 67.708(b)(3)-(4).

On September 3, 2026, the Requester filed an appeal with the Office of Open Records ("OOR"), challenging the denial and stating grounds for disclosure. The OOR invited both parties to supplement the record and directed the District to notify the OOR if any third parties have a direct interest in the appeal. 65 P.S. § 67.1101(c).

On September 18, 2026, the District submitted a position statement, reiterating its argument and arguing that the requested records do not exist in the format and for the timeframe requested. In support, the District submitted a statement made under the penalties of unsworn falsification to authorities by Paul Sanfrancesco, Director of Technology ("Sanfrancesco Attestation").

The District argues that the release of the responsive records are exempt from access because their disclosure would be reasonably likely to endanger computer security under Sections 708(b)(3) and (b)(4) of the RTKL. Section 708(b)(3) exempts from public disclosure:

> A record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include:
>
> (i) documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability n preventing, protecting against, mitigating or responding to a terrorist act[.]

65 P.S. § 67.708(b)(3)(i). Likewise, Section 708(b)(4) of the RKTL exempts from disclosure "[a] record regarding computer hardware, software and networks, including administrative or technical records which, if disclosed, would be reasonably likely to jeopardize computer security." 65 P.S. § 67.708(b)(4); *see California Borough v. Rothey*, 185 A.3d 456 (Pa. Commw. Ct. 2018) (holding that an agency must "offer more than speculation or conjecture to establish the security-related exceptions under the [RTKL]."). In order for a record to be exempt under Section 708(b)(4), it

"must be on the subject of computer hardware, software or networks." *See Monighan v. Pa. Dep't of Transp*., OOR Dkt. AP 2017-2428, 2018 PA O.O.R.D. LEXIS 331.

Here, the Sanfrancesco Attestation provides:[2]

> 8. I have served in the role of Director of Technology for the District for thirteen (13) years.
> …
> 10. Prior to coming to the District, I also served as the Director of Technology for the Archdiocese of Philadelphia and the Garnet Valley School District.
> …
> 12.Given my extensive background in both education and technology, I am acutely familiar with the cybersecurity threats that exist in a school environment.
>
> 13. In my role as Director of Technology for the District, I am directly responsible for overseeing and managing the District's technology infrastructure and ensuring network security.
>
> 14. I am also the most knowledgeable individual at the District about details regarding the District's internet content filtering and firewall systems, device management, and cybersecurity operations.
> …
> 16. I am intimately familiar with the District's network security architecture and the District's network configurations, capabilities, and limitations.
>
> 17. The District uses firewall equipment to manage and protect internal network resources from external threats.
>
> 18. The afore-mentioned technology is a critical component of the District's cybersecurity infrastructure, and it protects students and staff from harmful, inappropriate, or malicious online content, in addition to protecting the District's network from cyber threats, including malware, phishing, and ransomware attacks.
> …
> 26. … [T]he reports, logs, and data sought by the Requester reveal in detail which websites and domains are permitted or blocked by the District's content filtering system, which specific URLs have been accessed on District-issued devices, and the patterns of network traffic on the District's network as recorded by the [] content filtering system.
>
> 27. This information, in essence, constitutes a roadmap of the District's filtering rules, network architecture, and overall cybersecurity posture.

[2] The Attestation also provides that the requested records do not exist, and would need to be generated with the assistance of the District's third-party vendors. Sanfrancesco Attestation, ¶ 22. Even if records were created, data is only maintained for two weeks, a much shorter time frame than the 2.5 years sought in the Request. *Id.*, ¶ 23.

28. Creating reports that reveal which domains and websites are permitted or unblocked necessarily also discloses any gaps, exceptions, or allowances.

29. A malicious actor with knowledge of which domains are permitted could exploit those exceptions to serve malicious content through an allowed domain, thereby bypassing the filtering system entirely.

30. Conversely, knowing what is filtered implicitly reveals what is not filtered – effectively mapping the boundaries of the District's security coverage.

31. The network traffic logs, firewall logs, and web access logs sought in Subpart 3 are among the most sensitive records maintained by the District's IT department.

32. The District's firewall equipment manages and protects internal network resources from external threats from non-District actors.

33. The logs requested would, if disclosed, reveal the District's network architecture, traffic patterns, and routing paths.

34. These records record activity on a per-user level and only report the IP address of the device from which the activity was generated.

35. A sophisticated attacker could analyze this data to identify the District's network topology, determine which systems are most heavily used, locate potentially vulnerable endpoints, and plan a targeted cyberattack.

36. Network traffic logs are widely recognized in the cybersecurity community as critical security artifacts that should never be disclosed publicly.

37. In the aggregate, the data sought by the Requester reveals the scope and limitations of the District's content filtering system, and an individual with access to this data would understand not only what the District filters, but also the extent and effectiveness of that filtering and the traffic controls applied at the network perimeter.

38. In other words, the records, if disclosed, would render the District's security measures completely ineffective by showing precisely how they operate and what limitations or vulnerabilities exist.

39. The records sought in Subparts 1, 2, and 3 would essentially create a roadmap for a bad actor to develop a detailed view of the District's cybersecurity system, and completely circumvent the policies the District has put in place to protect its network security.

40. Additionally, the records would expose specific user browsing activity and behaviors as the filter is applied to the user, and not the device they are using.

> 41. From a security perspective, sharing this information with this level of detail could further expose the District to unnecessary additional threats and potential weaknesses in the District's current security posture.
>
> 42. The cybersecurity threats to school districts is severe and growing.
>
> 43. School districts are increasingly targeted by ransomware, phishing, data exfiltration, and other cyberattacks, in part because school districts maintain large volumes of sensitive student and financial data and often have limited cybersecurity resources relative to the value of the data they protect.
>
> 44. Any disclosure that weakens the District's security posture puts students' personally identifiable information, financial records, employee data, and critical educational systems at risk.
>
> 45. A sophisticated attacker would be able to use the information contained in the records sought in Subparts 1, 2, and 3 to craft phishing and other attacks targeting District staff or students, identify vulnerable endpoints on the District's network, develop exploits targeting specific weaknesses in the District's systems, or serve malicious content through domains that the District's system is configured to permit.

The OOR finds the evidence provided by Director Sanfrancesco to be credible and adopts his security evaluation and risk assessments concerning information related to the responsive records and computer security. *See Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 180 (Pa. Commw. Ct. 2019). Based on this evidence, and in the absence of evidence to the contrary, the District has demonstrated that disclosure of the requested records is reasonably likely to jeopardize computer security. *See, e.g., Holloway v. Pa Dept. Gen. Serv*., OOR Dkt. AP 2023-1476, 2023 PA O.O.R.D. LEXIS 1665 (holding that where the agency provided detailed evidence that the information from invoices withheld was on the subject of computer hardware, software, or networks and articulated threats that would arise out of the public disclosure of such information, the information was exempt under Section 708(b)(4) of the RTKL); *Campbell v. Pa. Interscholastic Athletic Ass'n*, 268 A.3d 502 (Pa. Commw. Ct. 2021) (the preponderance of the evidence standard, which is the lowest evidentiary standard, is tantamount to a "more likely than

not" inquiry). Accordingly, the District has met its burden of proving that disclosure of the requested records would be reasonably likely to jeopardize computer security. *See* 65 P.S. § 67.708(a)(1).

For the foregoing reasons, the appeal is **denied**, and the District is not required to take any further action. This Final Determination is binding on all parties. Within thirty days of the mailing date of this Final Determination, any party may appeal to the Chester County Court of Common Pleas. 65 P.S. § 67.1302(a). All parties must be served with notice of the appeal. The OOR also shall be served notice and have an opportunity to respond according to court rules as per Section 1303 of the RTKL, 65 P.S. § 67.1303, but as the quasi-judicial tribunal that adjudicated this matter, the OOR is not a proper party to any appeal and should not be named as a party.[3] All documents or communications following the issuance of this Final Determination shall be sent to oor-postfd@pa.gov. This Final Determination shall be placed on the website at: http://openrecords.pa.gov.

FINAL DETERMINATION ISSUED AND MAILED: October 5, 2026

/s/ Blake Eilers
Blake Eilers, Esq.
Senior Appeals Officer

Delivered via e-file portal to: Todd Shepherd; David Francella; Alicia S. Luke, Esq.

[3] *Padgett v. Pa. State Police*, 73 A.3d 644, 648 n.5 (Pa. Commw. Ct. 2013).