pennsylvania
OFFICE OF OPEN RECORDS

FINAL DETERMINATION

IN THE MATTER OF	:	
	:	
TODD SHEPHERD and BROAD AND LIBERTY,	:	
Requester	:	
	:	
v.	:	**Docket No: AP 2026-3662**
	:	
ROSE TREE MEDIA SCHOOL DISTRICT,	:	
Respondent	:	

FACTUAL BACKGROUND

On July 15, 2026, Todd Shepherd and Broad and Liberty (collectively "Requester") submitted a request ("Request") to the Rose Tree Media School District ("District") pursuant to the Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101 *et seq*., seeking:

> [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 [D]istrict-issued devices 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 district-issued devices for the same period.

> [4.] All communications — including email, text, or internal messaging — sent or received by the Superintendent, the [D]istrict's Chief Technology or Chief Information Officer, or any administrator with primary responsibility for the [D]istrict's technology infrastructure, referencing the effectiveness, failure, or bypass of the [D]istrict's internet content filtering system for the period January 1, 2024 through the date of this [R]equest.
>
> [5.] All contracts or service agreements between the [D]istrict and any internet content filtering vendor currently or previously in effect.
>
> [6.] All reports, presentations, or analyses regarding student internet usage or screen time presented to the school board or any [D]istrict committee for the same period.
>
> [7.] …[A] copy of all documents that show payments from the [District] to the law firm Fox Rothschild from Jan[uary] []1, 2020, to present. I request a copy of all invoices and letters of engagement between the [D]istrict and Fox Rothschild for the same date range.
>
> [8.] …[A] copy of the [D]istrict's [RTKL] log from Jan[uary] []1, 2020, to present.

On August 24, 2026, following a thirty-day extension during which to respond, 65 P.S. § 67.902(b), the District partially granted the Request and provided partial records responsive to Items 5 and 7 of the Request.[1] The District also denied portions of the Request, claiming the release of records responsive to Items 1 through 3 would create a reasonable likelihood of endangering the security of the District's information storage system and computer security, 65 P.S. §§ 67.708(b)(3), (b)(4), and asserting that records responsive to Items 4, 6, and 8 do not exist in the District's possession, custody or control. The District also asserts that records responsive to Item 1 through 3 would be tied to student accounts or devices, and as such, would be protected under the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g.

On September 3, 2026, the Requester filed an appeal with the Office of Open Records ("OOR"), challenging the denial of Items 1 and 3. The OOR invited both parties to supplement

[1] As the Requester does not challenge the District's response to Items 2, 4 and 5-8, including any redactions made pursuant to 65 P.S. § 67.708(b)(6)(i)(A), 65 P.S. § 67.708(b)(11), and 65 P.S. § 67.708 (b)(30), those Items and the District's response thereto, will not be further addressed herein.

the record and directed the District to notify the OOR if any third parties have a direct interest in this appeal. 65 P.S. § 67.1101(c).

On September 18, 2026, the District submitted a position statement,[2] reiterating its basis for denial of Items 1 and 3 of the Request based upon Sections 708(b)(3) and (4) of the RTKL. In support of the District's position, the District submitted two attestations made subject to the penalties under 18 Pa. C.S. § 4904, relating to unsworn falsifications to authorities, authored by Vanessa Scott, Ed.D. ("Scott Attestation"), the District's Director of Management Services and Agency Open Records Officer ("AORO"), and Ron Harris ("Harris Attestation"), the District's Network Specialist.

LEGAL ANALYSIS

The District is a local agency subject to the RTKL. 65 P.S. § 67.302. Records in the possession of a local agency are presumed to be public, unless exempt under the RTKL or other law or protected by a privilege, judicial order or decree. *See* 65 P.S. § 67.305. As an agency subject to the RTKL, the District is required to demonstrate, "by a preponderance of the evidence," that records are exempt from public access. 65 P.S. § 67.708(a)(1). Preponderance of the evidence has been defined as "such proof as leads the fact-finder … to find that the existence of a contested fact is more probable than its nonexistence." *Pa. State Troopers Ass'n v. Scolforo*, 18 A.3d 435, 439 (Pa. Commw. Ct. 2011) (quoting *Pa. Dep't of Transp. v. Agric. Lands Condemnation Approval Bd.*, 5 A.3d 821, 827 (Pa. Commw. Ct. 2010)).

The District argues that the release of the responsive records are exempt from access because release of these records 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:

[2] On September 16, 2026, the District initially submitted a position statement; however, on September 18, 2026 the District submitted an amended position statement to correct a case citation.

> 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.

In support of the District's position, the Harris Attestation provides the following:

1. […]I am responsible for managing the District's technology infrastructure, including network security, internet content filtering systems, firewall administration, student device management, and cybersecurity operations.

2. I have extensive professional experience in information technology and cybersecurity in the K-12 education environment. […]

3. I am intimately familiar with the District's network security architecture, FortiGate firewall, LineWize Content Filter, their configurations, capabilities, and limitations. The District uses FortiGate firewall equipment to manage and protect internal network resources from external/internet-based threats. The [D]istrict segments internal traffic into subnetworks, allowing specific firewall traffic policies to be applied to different groups of devices. The [D]istrict does not apply web filtering policies to [D]istrict-issued devices using the FortiGate firewall; the firewall policies operate at the network level and only allow traffic based on specific ports necessary for internet access. The District's LineWize Content Filter is a user-based web filtering agent installed on [D]istrict-issued devices (PCs, MacBooks, iPads, and Chromebooks). This filtering system is cloud-based and allows filtering policies to be set at the group or user level.

The agent/extension installed on [D]istrict issued devices forwards web activity initiated by the logged-in user to the cloud-based system where filtering policies are applied. This technology is a critical component of the [D]istrict's cybersecurity infrastructure. It serves the dual purpose of protecting students and staff from harmful, inappropriate, or malicious online content and protecting the District's network from cyber threats, including malware, phishing, and ransomware attacks.

[…]

6. Based on my review and my professional expertise, I have determined that release of the records responsive to Items 1 and 3 would endanger the security of the District's computer systems and network. The reports, logs, and data sought by the Requester reveal in detail which websites and domains are permitted or blocked by the District's LineWize Content Filter, which specific URLs have been accessed on [D]istrict-issued devices, and the patterns of network traffic on the District's network as recorded by the FortiGate firewall and LineWize system. This information constitutes a roadmap of the District's filtering rules, network architecture, and overall cybersecurity posture. My specific concerns are set forth in the following paragraphs.

7. The reports and dashboards generated by the District's LineWize Content Filter (Item 1) reveal which domains and websites are permitted or unblocked. This information discloses the District's user-and group-based filtering rules, including any gaps, exceptions, or allowances in the LineWize configuration. A malicious actor with knowledge of which domains are permitted could exploit those exceptions to serve malicious content through an allowed domain (a technique known as "domain fronting" or "trusted-site abuse"), thereby bypassing the filtering system entirely. Conversely, knowing what is filtered implicitly reveals what is *not* filtered – effectively mapping the boundaries of the District's security coverage.

8. The network traffic logs, FortiGate firewall logs, LineWize logs, and web access logs sought in Item 3 are among the most sensitive records maintained by the District's IT department. FortiGate firewall equipment manages and protects internal network resources from external/internet-based threats, and the District segments internal traffic into subnetworks so that different traffic policies can be applied to different groups of devices. Logs from the FortiGate firewall and LineWize system reveal the District's network architecture, traffic patterns, and routing paths. The LineWize system records activity on a per-user level and only reports the IP address of the device from which the activity was generated. The LineWize system retains user history for up to three months. 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.

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

9. In the aggregate, the data sought by [the Requester] reveals the scope and limitations of the District's LineWize Content Filter and the relationship between the LineWize filtering layer and the FortiGate firewall. An actor 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. This is analogous to publishing the combination to a safe – if it renders the security measure ineffective by revealing precisely how they operate and where their boundaries lie.

10. Sharing all logs and reports from the FortiGate firewall would essentially be creating a roadmap for the [R]equest[e]r to develop a detailed view of our internal network segmentation, IP addressing schemes, upstream provider routes, and the policies we have configured to manage them. Additionally, sharing logs from the Line Wize content filter would expose specific user browsing activity and behaviors as the filter is applied to the user not the device they are using. From a security perspective sharing this information with this level of detail could further expose the [D]istrict to unnecessary additional threats and potential weaknesses in our current security posture.

11. The cybersecurity threat landscape for K-12 school districts is severe and growing. School districts are increasingly targeted by ransomware, phishing, data exfiltration, and other cyberattacks. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have repeatedly issued advisories warning that K-12 institutions are high-value targets for cybercriminals, 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. Any disclosure that weakens the District's security posture puts student personally identifiable information, financial records, employee data, and critical educational systems at risk.

12. I receive messages and updates frequently from the DCIU, IU13, and other districts about cyber security breaches or threats that are impacting schools. I am aware that the Delaware County Courthouse suffered a significant breach that took their systems down for weeks as recently as June 2026. The threat landscape in the age of AI is literally changing by the minute which requires us to be as vigilant as possible to ensure we are protecting our network and user data as much as possible. Sharing historical network and content filtering logs would expose the very data we are trying to hard to protect.

13. A sophisticated attacker could use the information contained in the records sought by [the Requester] to craft phishing attacks targeting District staff or students, identify vulnerable endpoints on the District's network, develop

exploits targeting specific weaknesses in the LineWize Content Filter or FortiGate firewall, or serve malicious content through domains that the District's filtering system is configured to permit. The risk is not theoretical – K-12 school districts across the country have experienced devastating cyberattacks in recent years, resulting in data breaches, ransomware incidents, disruption of educational operations, and significant financial losses and one of my primary duties at the District is minimizing that risk. The release of this information would do the opposite.

14. Our systems are under constant pressure from attacks and adversaries trying to gain access to staff and student data. Most of our users receive phishing and scam emails daily and some have been received by students. Our systems monitor and alert us on account compromises and password spray attacks that happen frequently due to our user account and password data being exposed through third party data breaches. This is a frequent conversation I have with other IT professionals in every district across Delaware and Chester Counties. The LineWize content filter and Firewall systems are a critical part of the systems we use to not only maintain CIPAA compliance but to do as much as we possibly can to protect our users from malicious and possibly destructive content. Releasing user based logs and system would violate that best practice.

Under the RTKL, a sworn affidavit or statement made under the penalty of perjury may serve as sufficient evidentiary support. *See Sherry v. Radnor Twp. Sch. Dist.*, 20 A.3d 515, 520-21 (Pa. Commw. Ct. 2011); *Moore v. Office of Open Records*, 992 A.2d 907, 909 (Pa. Commw. Ct. 2010). In the absence of any evidence that the District has acted in bad faith, "the averments in the [attestation] should be accepted as true." *McGowan v. Pa. Dep't of Envtl. Prot.*, 103 A.3d 374, 382-83 (Pa. Commw. Ct. 2014) (citing *Office of the Governor v. Scolforo*, 65 A.3d 1095, 1103 (Pa. Commw. Ct. 2013)).

To demonstrate that a record is exempt under one of the security exemptions under the RTKL, an agency must provide detailed evidence showing how disclosure of the information is likely to present such a threat. *Sheckler v. Pa. Dept. of State*, OOR Dkt. AP 2022-0492, 2022 PA O.O.R.D. LEXIS 1175 (holding that the SURE election system user guide was exempt under Sections 708(b)(3) and (4) where the agency presented the professional opinions of experts in election security and cybersecurity to demonstrate the threat to public infrastructure and computer

security). In this instance, the District's attestation is authored by Mr. Harris, who serves as the District's Network Specialist, an individual with twenty-six years of experience with information technology in the K-12 education environment. Mr. Harris details the dangers in releasing the responsive records to the public, including the severe and growing threats faced by school districts, and describes that the District's LineWize content filters and Firewall systems are "a critical part of the system [the District] use[s] to not only maintain CIPAA compliance but to do as much as we can to protect our users from malicious and possibly destructive content." Harris Attestation ¶ 14. The District's evidence adequately explains in sufficient detail how the responsive records are used to "craft phishing and other attacks targeting District staff or students" as it pertains to the disclosure of the responsive records and detailing the risk of "data breaches, ransomware incidents, disruption of educational operations, and significant financial losses." Harris Attestation ¶ 13. Further, the subject matter of the Request clearly seeks records pertaining to analysis of the District's internet content filtering system, and network information; therefore, it is not unreasonable to believe that responsive records would house pertinent computer security information.

The OOR finds the evidence provided by Mr. Harris to be credible and adopts his security evaluation and risk assessments concerning information related to the responsive records and computer security. *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 180 (Pa. Commw. Ct. 2019). Accordingly, in the absence of evidence to the contrary, the OOR can conclude, by a preponderance of the evidence, that the District has demonstrated that it properly withheld records that would 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).[3]

CONCLUSION

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 Delaware 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 as per Section 1303 of the RTKL; however, as the quasi-judicial tribunal adjudicating this matter, the OOR is not a proper party to any appeal and should not be named as a party.[4] 65 P.S. § 67.1303. 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 OOR website at: http://openrecords.pa.gov.

FINAL DETERMINATION ISSUED AND MAILED: October 5, 2026

/s/ Lyle Hartranft

LYLE HARTRANFT, ESQ.
APPEALS OFFICER

Sent via OOR portal only to: Todd Shepherd; Vanessa Scott, AORO; Kyle Berman, Esq.

[3] Because the OOR finds that these records are exempt from access pursuant to Sections 708(b)(3) and 708(b)(4) of the RTKL, the OOR need not reach the District's alternative grounds for denying access to these records. *See Jamison v. Norristown Bor. Police Dept*., OOR Dkt. AP 2011-1233, 2011 PA O.O.R.D. LEXIS 927.
[4] *Padgett v. Pa. State Police*, 73 A.3d 644, 648 n.5 (Pa. Commw. Ct. 2013).