pennsylvania
OFFICE OF OPEN RECORDS

FINAL DETERMINATION

IN THE MATTER OF	:	
	:	
TODD SHEPHERD AND BROAD AND LIBERTY,	:	
Requester	:	
	:	**Docket No: AP 2026-3852**
v.	:	
	:	
BENSALEM TOWNSHIP SCHOOL DISTRICT,	:	
Respondent	:	

FACTUAL BACKGROUND

On July 15, 2026, Todd Shepherd, a reporter with Broad and Liberty (collectively "Requester"), submitted a request ("Request") to Bensalem Township 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 [D]istrict-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.

I also request a copy of all documents that show payments from the [District] to the law firm Fox Rothschild from Jan 01, 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.

I also request a copy of the [D]istrict's [RTKL] log from Jan 01, 2020, to present.

On August 21, 2026, following a thirty-day extension, 65 P.S. § 67.902(b), the District granted the Request in part, providing records responsive to Items 1 and 5 of the Request, check register reports, and a copy of the District's RTKL log. The District also denied the Request in part, asserting that records responsive to Item 3 pose a security risk to the District if diclosed, and Item 4 of the Request is insufficiently specific. 65 P.S. § 67.703. The District further asserts that records responsive to Items 2 and 6 of the Request do not exist in its possession, custody or control.

On September 11, 2026, the Requester appealed to the Office of Open Records ("OOR"), challenging the District's denial of "computer logs and [D]istrict emails" and stating grounds for disclosure.[1] 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 30, 2026, the District submitted a position statement in response to the appeal. Specifically, the District clarifies that records responsive to Item 3 of the Request do not

[1] The Requester's only challenge on appeal is the District's denial of Items 3 and 4 of the Request. As such, the OOR need not address other issues in this Final Determination. *See Dep't of Corr. v. Office of Open Records*, 18 A.3d 429 (Pa. Commw. Ct. 2011) (issues not raised on appeal are waived).

exist for the timeframe specified in Request, but even so, such records would be exempt from access because release of these records would be reasonably likely to endanger computer security. 65 P.S. § 67.708(b)(4). Concerning Item 4 of the Request, rather than arguing specificity, the District has identified 3 responsive email chains. The District asserts that the email chains constitute internal, predecisional deliberations, noncriminal investigations, and contain the names of minors, and information protected under the Family Educational Rights and Privacy Act ("FERPA"). 65 P.S. § 67.708(b)(10); 65 P.S. § 67.708(b)(17); 65 P.S. § 67.708(b)(30); 20 U.S.C. § 1232g, *et seq*. Finally, the District asserts that text messages responsive to Item 4 of the Request do not exist in its possession, custody or control. In support of its position, the District submitted the attestations of Kurt Von Schwedler ("Von Schwedler Attestation") Network Engineer for the District; Victoria Velazquez ("Velazquez Attestation"), Interim Superintendent for the District; and Donna Minnigh ("Minnigh Attestation"), Acting Assistant to the Superintendent.[2]

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)).

[2] These Attestations are made subject to penalties under 18 Pa. C.S. § 4904, relating to unsworn falsifications to authorities.

1. Records responsive to Item 3 of the Request are exempt from access pursuant to Section 708(b)(4) of the RTKL

As a preliminary matter, the District asserts that "traffic logs, firewall logs, and web access logs maintained by the District are retained only for approximately one day," and explains that "[t]he logs are continuously deleted because of the massive amounts of data generated by the District each day." Von Schwedler Attestation ¶ 8. As such, responsive log records for the specified timeframe do not exist. *Id*. Nevertheless, the District argues that such records would be exempt from access because release of these records would be reasonably likely to endanger computer security.

Section 708(b)(4) of the RTKL 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; *see also Abraham v. Sch. Dist. of Phila.*, OOR Dkt. AP 2012-0070, 2012 PA O.O.R.D. LEXIS 47; 1 Pa.C.S. § 1903 (under the rules of statutory construction, "[w]ords and phrases shall be construed according to rules of grammar and according to their common and approved usage"). In support of the District's position, the Von Schwedler Attestation states, in part:

> 9. [T]hese logs reveal all the devices connected to the District's servers, which include not only District-issued devices but personal devices such as cell phones, Amazon Echos, and smartwatches belonging to staff members and students. On any given school day, approximately 10,000 devices, both [D]istrict-issued and personal, are connected to the District's network.

10. Moreover, the traffic logs, firewall logs, and web access logs contain information which includes IP addresses, sensitive outbound data, and sensitive inbound data. The information contained in these logs can reveal points of entry in the District's firewall to bad actors or that can identify web-based services which may contain financial information or other high-value target data (mean data for which an agency may be more willing to pay a ransom) or that can identify learning platforms that could hamper or even cripple a school district's ability to conduct classes or its business functions.

11. If a bad actor were to gain access to the District's traffic logs, firewall logs, and web access logs, the bad actor could potentially identify specific web-based servers. The bad actor would be able to quickly pinpoint what servers maintain the data that is most valuable to the District, meaning account numbers, sensitive personal staff and student data, or the data most critical to school functioning and most likely to reap the largest ransom. A bad actor who also has access to stolen employee credentials through a successful phishing or spear could force their way into the most "valuable" servers because the traffic logs, firewall logs, and web access logs have identified their locations. Without the traffic logs, firewall logs, and web access logs a bad actor with stolen credentials would need to rely on a laborious trial and error process.

12. Further, once a school district or government agency has been hit with a ransomware attack, the stolen data will not be available to that agency until a ransom is paid, and the bad actor may sell that data to another bad actor, regardless of whether the ransom is paid. I am aware of multiple ransomware attacks that have occurred against school districts in Pennsylvania over recent years that disrupted school days and forced closures, as well as one against the Pennsylvania Attorney General's Office last year.

13. A bad actor can also use the information in these logs to interfere with specific educational platforms used in the classroom and interfere with the proper functioning of the school. Earlier this year, a hacker group attacked Canva, a cloud-based learning platform which impacted thousands of schools. These logs can be used to determine whether a school district uses a particular web-based platform and exploit vulnerabilities on that platform to cyberattack, or plan an attack, in a school district's cloud-based learning programs. In this case, the District was not a Canva user, however, I am aware of nearby school districts that were impacted. Additionally, identification of platforms used by the District can be used by rogue actors to create highly-personalized spear phishing attacks to try and steal employee credentials.

14. The IP addresses in the logs can also inform a bad actor how to interfere with a school district's internet service. A bad actor can engage in a denial of services attack where it overloads the network appliance providing internet access to school. This attack uses all of a district's bandwidth and makes accessing any internet-based applications extremely slow, if not impossible, to access. I am

> aware of a nearby school district that was subject to this kind of attack within the last five years.

Under the RTKL, an affidavit or statement made under penalty of perjury may serve as sufficient evidentiary support. *See Sherry v. Radnor Twp. Sch. Dist.*, 20 A.3d 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 competent evidence that the District 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)).

The OOR finds the evidence provided by Mr. Von Schwedler to be credible and adopts his security evaluation and risk assessments concerning any records responsive to Item 3 of the Request and computer security. *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 180 (Pa. Commw. Ct. 2019). Accordingly, the OOR can conclude, by a preponderance of the evidence, that the District has demonstrated that disclosure of records responsive to Item 3 of the Request 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 withheld information from invoices 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).

2. The District has demonstrated that emails responsive to Item 4 of the Request are exempt from access pursuant to Section 708(b)(17) of the RTKL

The District asserts that 3 email[3] chains responsive to Item 4 of the Request are exempt from access because they relate to noncriminal investigations. Section 708(b)(17) of the RTKL exempts from disclosure records of an agency "relating to a noncriminal investigation," including, "complaints submitted to an agency," "[i]nvestigative materials, notes, correspondence and reports" and "[a] record that, if disclosed, would…[r]eveal the institution, progress or result of an agency investigation." 65 P.S. § 67.708(b)(17)(i)(ii); 65 P.S. § 67.708(b)(17)(vi)(A). In order for this exemption to apply, an agency must demonstrate that "a systematic or searching inquiry, a detailed examination, or an official probe" was conducted regarding a noncriminal matter. *See Pa. Dep't of Health v. Office of Open Records*, 4 A.3d 803, 810-11 (Pa. Commw. Ct. 2010). Further, the inquiry, examination, or probe must be "conducted as part of an agency's official duties." *Id*. at 814; *see also Johnson v. Pa. Convention Ctr. Auth.*, 49 A.3d 920 (Pa. Commw. Ct. 2012). An official probe only applies to noncriminal investigations conducted by agencies acting within their legislatively granted fact-finding and investigative powers. *Pa. Dep't of Pub. Welfare v. Chawaga*, 91 A.3d 257 (Pa. Commw. Ct. 2014). To hold otherwise would "craft a gaping exemption under which any governmental information-gathering could be shielded from disclosure." *Id*. at 259.

The OOR has previously held that school districts have a legislatively granted authority to conduct noncriminal investigations where it concerns the welfare of its students. *See*, *e.g.*, *Haring v. Central Bucks Sch. Dist.*, OOR Dkt. AP 2020-0340, 2020 PA O.O.R.D. LEXIS 1851 (holding that records related to the school district's investigation of bullying allegations related to the girls'

[3] While the issues on appeal have been limited to "computer logs and [D]istrict emails," the District has provided sufficient evidence to affirm that no responsive text messages were located. Von Schwedler Attestation ¶ 26; Velazquez Attestation ¶ 5; Minnigh Attestation ¶ 7.

lacrosse program was conducted pursuant to its legislatively granted authority); *Davies v. Leechburg Area Sch. Dist.*, OOR Dkt. AP 2016-1110, 2016 PA O.O.R.D. LEXIS 1335 (holding that pursuant to the Public School Code, the district had the duty and authority to investigate allegations of hazing concerning the boys' basketball program); *Lederach v. Norwin Sch. Dist.*, OOR Dkt. 2015-1310, 2015 PA O.O.R.D. LEXIS 1308 (holding that an investigation related to alleged harassment was a noncriminal investigation because it was conducted under the authority of the School Code). As such, the District has the legislatively granted authority to conduct noncriminal investigations.

Here, the Von Schwedler Attestation affirms and provides sufficient evidence to demonstrate that the District located 3 responsive email chains that each detail the District's investigation into complaints and concerns about students being able bypass filters and gain access into certain blocked websites, and what investigative steps the District intended to take. Von Schwedler Attestation ¶¶ 23-25. Based on the evidence provided, disclosure of these emails would reasonably reveal "complaints submitted to an agency," "[i]nvestigative materials, notes, correspondence and reports," and "…the institution, progress or result of an agency investigation." 65 P.S. § 67.708(b)(17)(i)(ii); 65 P.S. § 67.708(b)(17)(vi)(A). Accordingly, the OOR finds that records responsive to Item 4 of the Request relate to a noncriminal investigation and are exempt from access pursuant to Section 708(b)(17) of the RTKL.[4]

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

[4] Because the OOR finds that these records are exempt from access under Section 708(b)(17) 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.

date of this Final Determination, any party may appeal to the Bucks 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. 65 P.S. § 67.1303. 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.[5] 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 22, 2026

/s/ Tope L. Quadri

_____

TOPE L. QUADRI
APPEALS OFFICER

Sent to via portal to: Todd Shepherd
Dr. Victoria Velazquez, AORO
Joanna Dombrowski, Esq.

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