CAUSE NO. 348-362718-25

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY,	§	**IN THE DISTRICT COURT OF**
Plaintiff,	§	
v.	§	**348TH JUDICIAL DISTRICT**
GRAPEVINE-COLLEYVILLE INDEPENDENT SCHOOL DISTRICT,	§	
Defendant.	§	**TARRANT COUNTY, TEXAS**

DEFENDANT'S RESPONSE TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

Pursuant to Tex. R. Civ. P. 166a and the parties' Rule 11 agreement, Defendant Grapevine-Colleyville Independent School District ("GCISD"), files the following response to Plaintiff Knight First Amendment Institute at Columbia University's Motion for Summary Judgment.

I. INTRODUCTION

1. In March 2023 Plaintiff Knight First Amendment Institute at Columbia University ("Knight") sent a Texas Public Information Act request to GCISD asking for "records related to the District's use of surveillance systems to monitor students' activity on school-issued devises and software." Knight subsequently clarified and/or narrowed its request twice.

2. In response to Knight's requests, GCISD, as allowed by law, sought an Attorney General opinion on whether some or all of the requested information is exempt from disclosure under Tex. Gov't Code §552.139.[1] In three separate written decisions, the Attorney General determined that the majority of the requested records were exempt from disclosure under section

[1] Section 552.139(a) excepts from disclosure information that "relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network."

552.139 and that GCISD "***must*** withhold the information." In compliance with the Attorney General's decisions, GCISD has withheld several documents and has also produced 824 heavily redacted emails.

3. Not satisfied with the Attorney General's decisions and GCISD's subsequent withholding and redacted production, Knight filed the instant lawsuit seeking a writ of mandamus "compelling [GCISD] to disclose all responsive information." In support of its request for mandamus relief, Plaintiff's Original Petition alleges that:

> (1) "The information requested in the Original and Clarified Requests is not excepted from disclosure under the computer network security exception. See Tex. Gov't Code §552.139";
>
> (2) "Moreover, the information requested in the second part of Clarified Request II is presumptively public because GCISD did not timely request an opinion from the Attorney General that a TPIA exception applies to that information. See Tex. Gov't Code §552.302";[2]
>
> (3) "Finally, the Knight Institute is entitled to a fee waiver. Tex. Gov't Code §552.267(a)."

See Plaintiff's Original Petition, ¶¶ 42-44; see also Amended Petition, ¶¶ 46-48. Knight also asks for its attorney's fees. Id. at ¶ 47; ¶ 52.

4. In response, GCISD has filed a general denial and asserted the following two affirmative defenses:

> (1) The redacted emails produced by Defendant to Plaintiff about which Plaintiff complains of in Plaintiff's Original Petition contain student information protected from disclosure by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g. Plaintiff lacks standing to challenge Defendant's redactions based on Defendant's FERPA determinations.

[2] Plaintiff's Amended Petition, ¶48, adds the additional allegation that "[t]he computer network security exception is neither a compelling justification *per se*, nor is it a compelling justification as applied to the records sought here."

(2) The Court may not assess costs of litigation and reasonable attorney's fees incurred by Plaintiff because Defendant acted in reasonable reliance on written decisions of the attorney general. See Tex. Gov't Code §552.323(a)(3).

5. On January 30, 2026, GCISD and Knight filed their respective cross motions for summary judgment.[3] By Rule 11 agreement, the parties agreed their respective responses would be filed on or before February 27, 2206. Consistent with the parties' agreement, GCISD now files its response to Knight's Motion for Summary Judgment.

II.
RESPONSE

A. Primary Response

6. GCISD's primary response is that Knight's summary judgment motion should be denied for all the reasons that GCISD's cross-motion should be granted. As shown in Defendant's Motion for Summary Judgment, the information sought by Knight is excepted from disclosure under Tex. Gov't Code §552.139(a) because it is information that "relates to … the design, operation, or defense of [GCISD's] computer network." Rather than re-state all of GCISD's arguments and authorities, GCISD refers the Court to Defendant's Motion for Summary Judgment, which is incorporated herein.

7. The remainder of this response will primarily address arguments in Knight's motion that are not already fully addressed in GCISD's motion.

B. Accepted Rules of Statutory Construction Favor GCISD's Interpretation of Section 552.032, Not Knight's Interpretation

8. Knight's motion posits that "[w]ith no court having interpreted section 552.139 to date, and with no statutory definition of 'computer network security,' traditional methods of statutory interpretation help to discern the intent of the Legislature in enacting the exception."

[3] The Court has set the motions for hearing by submission on March 11, 2026, at 8:00 a.m.

Plaintiff's Motion, p. 17. According to Knight's motion, "the plain and technical meaning of the provision's operative language, and the context of the exception's enactment, make clear that TPIA section 552.139 applies only to information that could facilitate unauthorized access to the District's network. … To begin, the technical meaning of the phrase 'information that relates to computer network security… or to the design, operation, or defense of a computer network,' TPIA section 552.139(a), means information that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access." Plaintiff's Motion, p. 18. Accepted rules of statutory construction, however, do not support Knight's adding to the plain language of section 552.139(a).

9. "Statutory construction is a question of law for the court to decide." *Tex. Dep't of Transp. v. Needham,* 82 S.W.3d 314, 318 (Tex. 2002). According to the Texas Supreme Court,

> When construing a statute, ***our primary objective is to determine the Legislature's intent which***, when possible, ***we discern from the plain meaning of the words chosen***.
>
> Ordinarily, the truest manifestation of what legislators intended is what lawmakers enacted, the literal text they voted on. If a statute is clear and unambiguous, we apply its words according to their common meaning without resort to rules of construction or extrinsic aids.
>
> We use definitions prescribed by the Legislature and any technical or particular meaning the words have acquired.[4] ***Otherwise, words not statutorily defined bear their common, ordinary meaning*** unless a more precise definition is apparent from the statutory context or the plain meaning yields an absurd result.

Maxim Crane Works, L.P. v. Zurich Am. Ins. Co., 642 S.W.3d 551, 557 (Tex. 2022) (internal citations omitted) (emphasis added). Stated another way,

[4] "[I]f a statute defines a term, a court is bound to construe that term by its statutory definition only." *Needham,* 82 S.W.3d at 318.

> When interpreting statutes we try to give effect to legislative intent. Legislative intent remains the polestar of statutory construction. However, ***it is cardinal law in Texas that a court construes a statute, first by looking to the plain and common meaning of the statute's words***. If the meaning of the statutory language is unambiguous, we adopt, with few exceptions, the interpretation supported by the plain meaning of the provision's words and terms. Further, if a statute is unambiguous, rules of construction or other extrinsic aids cannot be used to create ambiguity. …
>
> There are sound reasons we begin with the plain language of statute before resorting to rules of construction. For one, it is a fair assumption that the Legislature tries to say what it means, and therefore the words it chooses should be the surest guide to legislative intent. Also, ordinary citizens should be able to rely on the plain language of a statute to mean what it says. Moreover, when we stray from the plain language of a statute, we risk encroaching on the Legislature's function to decide what the law should be.

Fitzgerald v. Advanced Spine Fixation Sys., 996 S.W.2d 864, 865-66 (Tex. 1999) (internal citations omitted) (emphasis added).

10. "We presume the Legislature included each word in the statute with a purpose and that words not included were purposely omitted"; thus, "[w]e must give effect to every word and phrase if it reasonable to do so because we presume the Legislature used every word or phrase intentionally, with a meaning and a purpose." *Lippincott v. Whisenhunt,* 462 S.W.3d 507, 509 (Tex. 2015); *N.P. v. Methodist Hosp.,* 190 S.W.3d 217, 223 (Tex. App. – Houston [1st Dist.] 2006, pet. denied). Relevant to the statute here, "[i]t is the Legislature's responsibility to impose restrictions, if any, on the Open Records Act's unambiguous and unqualified language. Courts 'are not responsible for omissions in legislation,' but must 'take statutes as they find them.'" *Holmes v. Morales,* 924 S.W.2d 920, 925 (Tex. 1996) (quoting *Simmons v. Arnim,* 110 Tex. 309, 220 S.W. 66, 70 (Tex. 1920)); see also *Walker Cnty, ESD No. 3 v. City of Huntsville,* 658 S.W.3d 807, 815 (Tex. App. – Waco 2022, pet denied) ("If the text of a statute is unambiguous, we must take the Legislature at its word, respect its policy choices, and *not revise a statute under the guise of*

interpreting it.") (emphasis added). Notably, when giving effect to the Legislature's intent as expressed by the plain language of a statute, "[t]o determine a statutory term's common, ordinary meaning, we typically look first to their dictionary definitions and then consider the term's usage in other statutes, court decisions, and similar authorities." *Tex. State Bd. of Exam'rs of Marriage and Family Therapists v. Tex. Med. Ass'n,* 551 S.W.3d 28, 35 (Tex. 2017); *ISI Contr., Inc. v. Markham,* 647 S.W.3d 489, 494 (Tex. App. – San Antonio 2022, pet. denied). However, this does not include resorting to extrinsic aids like legislative history. *Id*.

11. Despite the statute's unambiguous language, Knight's motion nevertheless asks the Court to look to the legislative history of §552.139 to determine the Legislature's intent with respect to the three listed exceptions to disclosure. See Plaintiff's Motion, pp. 19-21. However, the Texas Supreme Court has repeatedly rejected this approach:

> The family urges us to consider various extrinsic construction aids that they contend confirm that the legislature intended their proposed construction. … As we have repeatedly explained, however, we do not rely on such extrinsic aids to construe unambiguous statutory language. *Sullivan,* 488 S.W.3d at 299 ("We, however, do not resort to extrinsic aides, such as legislative history, to interpret a statute that is clear and unambiguous.").[5]
>
> …
>
> The family notes, however, that section 311.023 of the Code Construction Act permits courts to consider a statute's legislative history "whether or not the statute is considered ambiguous on its face." See Tex. Gov't Code §311.023(3). Although this section may grant us legal permission, not all that is lawful is beneficial. Constitutionally, it is the courts' responsibility to construe statutes, not the legislature's. In fulfilling that duty, we do not consider legislative history or other extrinsic aides to interpret an unambiguous statute because the statute's plain language most reliably reveals the legislature's intent. *Sullivan,* 488 S.W.3d at 299. We have therefore "repeatedly branded" reliance on extrinsic aids as

[5] "And we will not rely on such extrinsic aids to create an ambiguity." *Tex. Health Presbyterian Hosp. of Denton v. D.A.,* 569 S.W.3d 126, 133 n. 8 (Tex. 2018) (citing *Fitzgerald,* 996 S.W.2d at 865-66).

> "'improper' and 'inappropriate' when statutory language is clear." *BankDirect,* 519 S.W.3d at 84.

Tex. Health Presbyterian Hosp. of Denton, 569 S.W.3d at 135-36. See also *Fleming Foods of Tex. v. Rylander,* 6 S.W.3d 278, 283-84 (Tex. 1999). Here, the language used by the Legislature in § 552.139(a) is clear and unambiguous, meaning this court should ***not***, as requested by Knight, improperly rely on extrinsic aids such as legislative history to construe the statute's plain language.

12. Turning to the unambiguous language used by § 552.139(a), five terms are particularly relevant to the Court's decision in this case: (1) "relates to," (2) "design," (3) "operation," (4) "computer network," and (5) "or." Each of these terms (none of which is defined in the statute) is discussed, in turn, as follows.

13. ***"Relates to"*** – The courts have held that the phrase "relates to," as used in other sections of the Public Information Act and in the dictionary, "is ***very broad,*** encompassing even information that would not be 'relevant,' in the evidentiary sense, during litigation." *B.W.B. v. Eans Indep. Sch. Dist.,* 2018 Tex. App. Lexis 223, * 19 (Tex. App. – Austin 2018, no pet.) (emphasis added). "The plain meaning of the phrase 'relates to' is 'to have a connection with, to refer to, or to concern.' In ordinary use, the phrase 'relates to' is ***very broad***." *City of San Antonio v. Abbott,* 432 S.W.3d 429, 432 (Tex. App. – Austin 2014, pet. denied) (emphasis added); see also *University of Tex. Law Sch. v. Texas Legal Found.,* 958 S.W.2d 479, 483 (Tex. App. – Austin 1997, no pet.) ("The [Texas Public Information] Act does not define the meaning of the words 'related to.' In this circumstance, we construe the words according to common usage. Ordinarily, the words 'related to' mean 'pertaining to,' 'associated with,' or 'connected with.' This definition is broader than the Foundation asserts.") (citing *Webster's Third New International Dictionary* 1916 (Philip E. Gove ed. 1986); *Black's Law Dictionary* 1288 (6th ed. 1990)); *Barron v. Shaisani,* 2021 Tex. App. Lexis

4367, * 35 (Tex. App. – Fort Worth 2021, pet. denied) ("The terminology 'relates to' is ***very broad*** in its ordinary usage.") (emphasis added).

14. The Austin Court of Appeals, after confirming that the phrase "relates to" is "very broad" when used by the Legislature in a statute, further observed that "[w]e must presume that the Legislature selected language in a statute with care and that every word or phrase was used with a purpose in mind. Thus, we must presume that the Legislature chose such a broad formulation [i.e., "relates to"] purposely." *City of San Antonio,* 432 S.W.3d at 432-33. See also *Tex. Dep't of Pub. Safety v. Abbott,* 310 S.W.3d 670, 675 (Tex. App. – Austin 2010, no pet.) ("The terminology 'relates to' is very broad in its ordinary usage, and we must presume that the legislature used such a broad formulation purposely. To conclude otherwise would be to judicially truncate the ordinary meaning of the words 'relates to.'"); *In re Tex. Dep't of State Health Servs.,* 278 S.W.3d 1, 4 (Tex. App. – Austin 2008, no pet.) ("By making confidential all reports, records, and information 'that relate to' cases or suspected cases of diseases [in the Health Code], the Legislature has chose to protect a broad range of information from public disclosure.").[6]

15. ***"Design"*** – "design" is defined in the dictionary as "a plan or protocol for carrying out or accomplishing something." *Merriam-Webster's Collegiate Dictionary* 313, 815 (10th ed.).

16. ***"Operation"*** – "operation" is defined in the dictionary as "a method or manner of functioning" / "a single step performed by a computer in the execution of a program." *Merriam-Webster's Collegiate Dictionary* 313, 815 (10th ed.).

[6] Knight's motion attempts to narrow the "very broad" phrase "relates to" used in § 552.139(a) by citing *Uvalde Consolidated Indep, Sch. Dist. v. Texas Tribune,* 720 S.W.2d 466 (Tex. App. – San Antonio 2025, no pet.). See Plaintiff's Motion, pp. 24-25. *Uvalde*, however, is of no help here. In *Uvalde*, the language used in a prior version of § 552.108 of the Public Information Act was interpreted by the courts as "broad and did not require a showing of any 'interference.' The Texas Supreme Court described it as a 'blanket exemption' … In 1997, the Legislature amended the exception to add the current 'interference' requirement …" 720 S.W.2d at 481-82. Unlike the provision involved in *Uvalde*, the Legislature has not amended § 552.139(a) to narrow the "very broad" "relates to" language. *Uvalde* is inapposite.

17. ***"Computer Network"*** – Knight's motion attempts to rely on its expert's explanation of the technical meaning of the phrase "computer network security" to argue that the exceptions to disclosure in §552.139(1) do not apply in this case. However, information that relates to "computer network ***security***" is only one of the three alternative exceptions listed in §552.139(a) – the third listed exception is for information that relates to "the design, operation, or defense of a computer network."[7] Notably, unlike the first exception for "computer network ***security***," this third alternative exception omits the word "security" after the words "computer network" (compare "computer network security" [first exception] with "computer network" [third exception]). This is important because "[w]e presume the Legislature included each word in the statute with a purpose and that words not included are purposely omitted." *Lippencott,* 462 S.W.3d at 509. In other words, the third exception in §552.139(a) is broader than the first exception in that it is not limited/narrowed by the word "security." However, Knight's motion fails to recognize this distinction, and improperly attempts to revise and add to the words used in §552.139(a) under the guise of interpreting it.

18. ***"Or"*** -- The Legislature's intentional use of the disjunctive participle "or" in Tex. Gov't Code §552.139(a) signifies a separation between three alternative exceptions from disclosure under the Public Information Act: (1) information that relates to "computer network security," ***or*** (2) information that relates to "restricted information under Section 2059.055," ***or*** (3) information that relates to "the design, operation, ***or*** defense of a computer network." See Tex. Gov't Code §552.139(a).

19. As stated by the Texas Supreme Court, "the Legislature's use of the disjunctive word 'or' is significant when interpreting statutes." *City of Lorena v. BMTP Holdings, L.P.*, 409

[7] Relevant to the "design or operation of GCISD's computer network," *student email accounts and internet access are part of GCISD's computer network*. See Berger Declaration, ¶ 5.

S.W.3d 634, 642 (Tex. 2013). "In its ordinary use the term 'or' is disjunctive,[8] and alternative in its effect." *Shell Petroleum Corp. v. Royal Petroleum Corp.*, 137 S.W.2d 753, 758 (Tex. 1940). "[T]he term 'or' is disjunctive and signifies a separation between two distinct ideas. It separates words or phrases in the alternative relationship, indicating that either of the separated words or phrases may be employed without the other. The use of the disjunctive usually indicates alternatives and requires that those alternatives be treated separately." *Jones v. State*, 175 S.W.3d 927, 932-33 (Tex. App. – Dallas 2005, no pet.); see also *Black v. Williams*, 2014 Tex. App. Lexis 11715, *7 (Tex. App. – Amarillo 2014, pet. denied) (same); *Heritage on the San Gabriel Homeowners Ass'n v. Tex. Comm'n on Envtl. Quality*, 393 S.W.3d 417, 427 (Tex. App. – Austin 2012, pet. denied) (same).

20. To summarize, the accepted rules of statutory construction do not support Knight's interpretation of the exceptions from disclosure in §552.139(a) as being limited to "information that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access." Plaintiff's Motion, p. 18. Rather, the plain language in §552.139(a) – including the "very broad" term "relates to," the disjunctive participle "or" to separate the three listed exceptions to disclosure, and the omission of the word "security" in the third alternative exception – shows that, as determined by the Attorney General (which is entitled to "great weight"), the information withheld by GCISD "relates to the design [or] operation of [GCISD's] computer network" under the statute.

[8] By comparison, "[t]he participle 'and' is conjunctive." *Cmty. Bank of Raymore v. Chesapeake Exploration, LLC*, 416 S.W.3d 750, 757 (Tex. App. – El Paso 2013, no pet.).

C. Knight's Motion and Its Expert's Report Fail to Address Section 555.032's Alternative Exception for Information That "Relates to" "the Design, Operation or Defense of a Computer Network"

21. As explained above, Tex. Gov't Code §552.139(a) – by the Legislature's intentional use of the disjunctive participle "or" – signifies a separation between three alternative exceptions from disclosure under the Public Information Act: (1) information that relates to "computer network security," ***or*** (2) information that relates to "restricted information under Section 2059.055," ***or*** (3) information that relates to "the design, operation, ***or*** defense of a computer network." See *Jones*, 175 S.W.3d at 932 (the term "or" is "disjunctive and signifies a separation between two distinct ideas. It separates words or phrases in the alternative relationship, indicating that either of the separated words or phrases may be employed without the other."). In other words, the word "or" in §552.139(a) means that the "design [or] operation" exception may be employed without reference to the alternative "computer network security" exception.

22. However, despite these three alternatives in §552.139(a) – *which are required to be "treated separately"*[9] – Knight's motion, relying on its expert's report (Exhibit T to Plaintiff's Motion), ***solely*** focuses on the "computer network security" exception, and ignores the alternative exception for information that "relates to" "the design [or] operation" of GCISD's computer network. See Plaintiff's Motion, pp. 17-21.

23. By contrast, as detailed in GCISD's summary judgment motion (see motion, ¶¶ 31-36) supported by its expert Kyle Berger's declaration and report (see Exhibit 1 hereto for convenience), student email accounts and internet access are part of GCISD's "computer network." See Berger Declaration, ¶ 5. Importantly, GCISD, as a recipient of federal funding, is subject to

[9] *Jones*, 175 S.W.3d at 933; *Black*, 2014 Tex. App. Lexis 11715 at *7; *Heritage on the San Gabriel Homeowners Ass'n,* 393 S.W.3d at 427.

the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763 (2000). CIPA was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. Critical to GCISD's "design or operation"[10] of its computer network, GCISD is required under CIPA to have blocking or filtering measures in place to address the following: access by minors to inappropriate matter on the internet; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking," and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and measures restricting minors' access to materials harmful to them.[11] See, e.g., *Parents, Families & Friends of Lesbians & Gays, Inc. v. Camdenton R-III Sch. Dist.*, 853 F.Supp.2d 888, 891 (W.D. Mo. 2012) (CIPA "requires schools to protect children using school computers from viewing visual depictions that are obscene, child pornography, or harmful to minors."); see also Berger Declaration, ¶ 5-6; Patterson Declaration, ¶ 2. Accordingly, to comply with CIPA, GCISD has retained the services of third-party vendors Lightspeed Solutions and Gaggle.Net to create and implement appropriate blocking and filtering measures for its computer network. Berger Declaration, ¶ 7; Patterson Declaration, ¶ 3-5. To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking

[10] Notably, the Act does not define the terms "design" or "operation" as used in § 552.139(a). The relevant dictionary definitions of these terms are: (1) "design" – "a plan or protocol for carrying out or accomplishing something," and (2) "operation" – "a method or manner of functioning" / "a single step performed by a computer in the execution of a program." *Merriam-Webster's Collegiate Dictionary* 313, 815 (10th ed.).

[11] GCISD's Policy CQ (LOCAL) and (LEGAL) incorporates the computer/internet safety requirements of CIPA. Barbaroux Declaration, ¶ 17 and Exhibit 19 thereto.

explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system. Berger Declaration, ¶ 8-17; Patterson Declaration, ¶ 4-5.[12] To summarize, GCISD has "designed" and is "operating" its "computer network" by using/installing/incorporating the Gaggle.Net and Lightspeed Solutions filtering systems into the school district's computer network. Thus, interpreting the term "relates to" as used in Government Code §552.139(a) ***"very broadly,"*** the word lists and analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's "computer network" and, therefore, should be excepted from disclosure to Knight pursuant to the plain language of Tex. Gov't Code §552.139(a).

24. Because the word lists and the analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's "computer network," Knight's request for a summary judgment requiring disclosure of this information should be denied.

D. Knight's Motion Fails to Address GCISD's FERPA-Based Redactions

25. One of GCISD's affirmative defenses is that Knight lacks standing to challenge its redactions of all student-identifying information pursuant to FERPA, 20 U.S.C. § 1232g. Knight's motion does not address this defense. To the extent required, in response to Knight's summary judgment request GCISD re-urges the argument in ¶¶ 41-45 of Defendant's Motion for Summary

[12] In addition to CIPA compliance, Lightspeed Solutions' filtering system also assists GCISD with complying with other student internet safety regulations such as Texas Senate Bill 1893 (effective September 1, 2023), which "prohibit[s] the use of certain social media applications and services on devices owned or leased by governmental entities."

Judgment that Knight lacks standing to challenge GCISD's redactions of student information under FERPA.

E. The Attorney General Correctly Found a Compelling Reason to Overcome Any Openness Presumption

26. Plaintiff's motion argues that GCISD should be required to produce the 824 redacted emails in unredacted form because it failed to request an Attorney General opinion within 10 business days of receiving Knight's request. See Plaintiff's Motion, pp. 25-26.

27. Because the 824 emails included keywords that correspond to the information the Attorney General had determined **must be withheld** in the Attorney General's August 31, 2023, decision, GCISD, without first seeking a third Attorney General opinion, redacted that information **the Attorney General had already determined must be withheld** pursuant to Section 552.139 when producing the emails with redactions. More specifically, these emails contain keywords, a notation about "threat type" and a note about why the incident was flagged, which is information that corresponds to the analytics reports responsive to the first part of Knight's clarified request, which the Attorney General determined **must be withheld** pursuant to Section 552.139. As discussed above, the redacted information in the 824 emails "relates to" the "operation or design" of GCISD's "computer network."

28. GCISD acknowledges that more than 10 business days passed between when the school district received Knight's request and when it sought the third Attorney General opinion specifically addressing the 824 emails.[13] However, as the Attorney General has determined in this case, Tex. Gov't Code §552.139 provides a compelling reason to overcome the presumption of openness and, as such, the Attorney General decided to evaluate the applicability of that section to

[13] Importantly, "We do not say that failure to properly give notice [pursuant to § 552.301] automatically results in disclosure [pursuant to § 552.302]." *Simmons v. Kuzmich*, 166 S.W.3d 342, 349 n.3 (Tex. App. – Fort Worth 2005, no pet.).

the emails submitted by GCISD past the 10-day deadline. See June 26, 2025, Attorney General Opinion, note 3; Tex. Atty. Gen. Op. OR2020-15920; Tex. Atty. Gen. Op. OR2018-02510. See also *Paxton v. City of Dallas*, 509 S.W.3d 247, 256 (Tex. 2017) ("We reject, however, the notion that statutory exceptions are categorically distinct from compelling reasons and that something more is always required to rebut the presumption that arises from a government body's failure to timely request an attorney general decision."); *Doe v. Tarrant County Dist. Attorney's Office*, 269 S.W.3d 147, 154 (Tex. App. – Fort Worth 2008, no pet.) ("The [Texas Public Information] Act itself provides a 'compelling reason' for a governmental actor to withhold information by imposing criminal penalties on any person who 'distributes information considered confidential under the terms of the Act.'").

29. Here, the "compelling reason" to overcome the presumption of openness is that, at the time of Knight's request, the Attorney General had **already determined** that this same information **must be withheld** by GCISD (or face potential criminal penalties). As such, there is no reason for the Court to not follow the Attorney General's decision in this case, a decision which should be given "great weight," and to find that GCISD properly withheld the redacted information in the 824 emails pursuant to Tex. Gov't Code §552.139 and that Tex. Gov't Code §552.302's presumption of openness does not require disclosure of the redacted information.

F. The Court Should Not Disturb GCISD's Decision to Not Waive Its Copy and Production Fees

30. Knight's motion argues that, as a matter of law, it is entitled to a fee waiver for the cost of processing information responsive to its request because disclosure of the requested information "would primarily benefit the general public." See Plaintiff's Motion, p. 27.

31. The Texas Public Information Act permits governmental entities such as GCISD to impose charges for the cost of copying records and, in certain circumstances, preparing them for

inspection. See Tex. Gov't Code §§ 552.261, .271. Relevant here, the governmental entity may also, in its *sole* discretion, grant a waiver or reduction of those charges. See Tex. Gov't Code § 552.267 (charges may be reduced or waived "***if*** the governmental body determines [to do so]"); 1 TAC § 70.1 ("the governmental body ***may*** grant a waiver or reduction for charges"). Importantly, however, whether to waive or reduce the charges in the present case is to be determined by GCISD *alone*, not the Court – as held by the Austin Court of Appeals, "Nowhere in the Act or the administrative code do we find any provision authorizing a court to limit the amount of reimbursement a governing body may seek from the requestor." *Thomas v. Cornyn*, 71 S.W.3d 473, 491 (Tex. App. – Austin 2014, pet. denied).

32. Here, GCISD has determined that it will not waive or reduce the $741.60 it charged to redact and produce the 824 emails responsive to Knight's request.[14] For example, regardless of Knight's intended use of the requested information, GCISD was nevertheless compelled to spend valuable school district resources to review for and redact FERPA protected student information in response to Knight's public information request, and has determined that waiver or reduction of these incurred costs is not warranted.[15] Critically, the Public Information Act does not authorize Knight's requested reversal of GCISD's statutorily allowed discretionary decision. See *Cornyn*, 71 S.W.3d at 491. The Court should therefore deny Knight's request for a summary judgment waiving GCISD's copy and production fees.

[14] See July 7, 2023, email from Ali Williams to Jennifer Jones, attached as Exhibit L to Plaintiff's Original Petition ("The District does not determine that the standard in Tex. Gov't Code Sec. 552.267(a) is met in this instance, and, therefore, will not waive or reduce the charges associated with the Knight First Amendment Institute's request.").

[15] See June 21, 2023, email from Ali Williams to Jennifer Jones, attached as Exhibit L to Plaintiff's Original Petition ("GCISD is not waiving its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law, including but not limited to personally identifiable information of students.").

G. The Court Should Deny Knight's Request for Attorney's Fees

33. Knight's petition asks for attorney's fees. See Amended Petition, ¶ 52. One of GCISD's affirmative defenses is that the Court may not assess attorney's fees under the Public Information Act because GCISD acted in reasonable reliance on written decisions of the Attorney General. Tex. Gov't Code §552.323(a)(3).

34. Knight's motion does not address either its attorney's fees request or GCISD's defense under section 552.323(a)(3). To the extent required, in response to Knight's summary judgment motion GCISD re-urges the argument in ¶¶ 44-46 of Defendant's Motion for Summary Judgment that Knight is not entitled to attorney's fees because GCISD acted in reasonable reliance on written decisions of the Attorney General.

III.
CONCLUSION

35. For these reasons and those set forth in Defendant's Motion for Summary Judgment, the Court should grant GCISD's Motion for Summary Judgment and deny Knight's Motion for Summary Judgment.

Respectfully submitted,

ABERNATHY, ROEDER, BOYD & HULLETT, P.C.

/s/ Charles J. Crawford
CHARLES J. CRAWFORD
State Bar No. 05018900
LUCAS C. HENRY
State Bar No. 24101901
1700 Redbud Blvd., Suite 300
McKinney, Texas 75069
Telephone: (214) 544-4000
Facsimile: (214) 544-4040
ccrawford@abernathy-law.com
lhenry@abernathy-law.com

ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that on February 27, 2026, a true and correct copy of Defendant's Response to Plaintiff's Motion for Summary Judgment has been served on all counsel of record via the Court's e-filing system.

/s/ Charles J. Crawford
Charles J. Crawford

EXHIBIT 1

CAUSE NO. 348-362718-25

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY,	§	**IN THE DISTRICT COURT OF**
Plaintiff,	§	
v.	§	**348TH JUDICIAL DISTRICT**
GRAPEVINE-COLLEYVILLE INDEPENDENT SCHOOL DISTRICT,	§	
Defendant.	§	**TARRANT COUNTY, TEXAS**

DECLARATION OF KYLE BERGER

1. My name is Kyle Berger. I am competent to make this declaration. The facts stated in this declaration are within my personal knowledge and are true and correct.

2. I am the Chief Technology Officer for Grapevine-Colleyville Independent School District ("GCISD"). As Chief Technology Officer my duties and responsibilities include directing the technology vision and strategy for the school district. I oversee the entire Technology Department, including network infrastructure, data management, cybersecurity, and operational support. A detailed description of my experience and qualifications is attached hereto as Exhibit 1.

3. The GCISD network is founded on a dedicated, high-capacity fiber optic backbone spanning over 45 miles, which provides resilient connectivity to all 24 instructional and operational facilities across the district community. This highly dense infrastructure supports a 1:1 digital learning environment, managing in excess of 45,000 unique device connections daily for over 16,000 assigned end-users (students and staff) across both comprehensive wired and high-density wireless systems. GCISD utilizes a robust hybrid operational model, maintaining two distinct physical data center facilities integrated seamlessly with multi-tenant cloud services, all managed with a critical 24/7/365 operational commitment to ensure continuous availability.

4. The network is engineered to support all critical district functions, including high-bandwidth instructional services, Voice over IP (VoIP) telephony, Safety and Security systems (surveillance and access control), and administrative Enterprise Resource Planning (ERP). To protect this mission-critical environment, the network employs a defense-in-depth approach utilizing top-tier firewall systems and comprehensive cybersecurity protection tools specifically compliant with student data regulations. The overall complexity of the network is significantly elevated by its capacity to support and securely manage global virtual learning platforms, necessitating sophisticated remote access infrastructure and bandwidth optimization for a geographically distributed user base.

5. GCISD, as a recipient of federal funding, is subject to the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763 (2000), which was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. This legislative requirement, which must be fulfilled for GCISD to remain eligible for federal funding, forces the adoption of core technology for GCISD's computer network, including content filtering. As GCISD's Chief Technology Officer, part of my duties and responsibilities include making sure that the design and operation of GCISD's computer network complies with CIPA – importantly, relevant to the design or operation of GCISD's computer network, ***student email accounts and internet access are part of GCISD's computer network***.

6. Critical to GCISD's design or operation of its computer network, GCISD is required under CIPA to have blocking or filtering measures in place to address the following: access by minors to inappropriate matter on the internet; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking," and other unlawful activities by minors online; unauthorized

disclosure, use, and dissemination of personal information regarding minors; and measures restricting minors' access to materials harmful to them. Beyond simple blocking, CIPA further requires schools to approve and publicly adopt an internet safety policy that covers restricting access to harmful content, ensuring safe communications, preventing unlawful online activities, and protecting student data. The filtering and monitoring systems provide the necessary auditing and enforcement tools to prove that this policy is actively implemented and adhered to across all devises used by students to access the internet.

7. As part of its efforts to comply with CIPA, GCISD has retained the services of third-party vendors Lightspeed Solutions and Gaggle.Net to create and implement appropriate blocking and filtering measures for its computer network. GCISD has service contracts with both Gaggle.Net and Lightspeed Solutions to provide filter/monitoring systems for GCISD's computer network. These systems are used as a tool to maximize the detection of unsafe, graphic, and/or obscene student communications and website content on school district devices. With Gaggle.Net, for example, search terms that implicate computer searches that indicate suicide ideation, or self-harm and threats of violence, or obscenity will result in email notifications to GCISD and immediate emergency phone calls if necessary. Similarly, Lightspeed Solutions monitors students' online activity on GCISD's computer network by utilizing web content filtering technology to protect students from harmful online content – in other words, Lightspeed Solutions' filter technology blocks obscene material on any devise using GCISD's computer network.[1] Notably, GCISD does ***not*** customize the lists of keywords or phrases to be monitored; rather, these lists are

[1] Content filtering solutions, such as Lightspeed Filter, are designed to function as the first line of defense, proactively preventing users from initiating connections with known malicious domains or downloading harmful content. Modern content filtering solutions has evolved from basic CIPA compliance tools into sophisticated security components akin to next-generation firewalls, capable of addressing the complex challenges of the contemporary threat landscape.

solely created and maintained by the district's computer service providers Lightspeed Solutions and Gaggle.Net. Both vendors consider their lists to be proprietary.

8. To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system.

9. When I say Lightspeed's filtering system "protects against malware and online threats," I mean it acts as a proactive gatekeeper that monitors, categorizes, and blocks high-risk traffic before exposure occurs. This reduces the likelihood of exploit delivery, phishing, or ransomware reaching endpoints and helps safeguard student data. How Lightspeed's filtering system helps defend K-12 (kindergarten – 12th grade) school environments against malware and cyberthreats includes:

- The system blocks and detects attempts to access or search for known or potentially malicious websites or services, including those hidden in encrypted traffic through TLS inspection. This reduces the attack surface and improves both cybersecurity and digital safety posture.
- It integrates threat-intelligence feeds from multiple industry sources, including PhishTank, vxIntel, Internet Watch Foundation (IWF), and MI6, paired with Lightspeed's proprietary AI categorization engine to detect new and emerging threat domains and proactively block newly registered or uncategorized sites.

- It uses devise-level SmartAgents and extensions on Windows, Chrome, Mac, and iOS so filtering and threat prevention apply whether district-owned devices are on the school network or off-campus/home.

- It detects and blocks access to domain-sharing and file-hosting services frequently used to distribute malware, phishing pages, or inappropriate material, reducing risk across both cybersecurity and student-safety vectors.

- It blocks anonymizers and high-risk networks like TOR outright and continues filtering VPN traffic since enforcement occurs at the device level.

- Beyond blocking malicious sites, the monitoring and reporting of our system detects users activity, such as suspicious search terms, to identify users who are attempting to circumvent protections, evade filtering, and put compliance and security at risk.

10. Solutions like Lightspeed's filtering system provide end-to-end content filtering, offering critical protection against cyber risks and distractions. The system employs device-level agents to ensure comprehensive coverage across platforms such as Windows, macOS, and Chrome/Edge browsers, meaning protection follows the device regardless of whether it is on or off the campus network. This focus on coverage across all devices is functionally an evolution of the filtering system into a network-aware Endpoint Detection and Response (EDR) component, ensuring that infections acquired off-network do not compromise the district network upon reconnection. The Filter leverages specific, cybersecurity-focused categories to prevent users from accessing harmful content, including features designed to trigger immediate "internet lockouts" when malicious or harmful content is detected. This capability supports the containment phase of incident response, limiting the potential spread of malware. The accuracy of blocking is enhanced by the incorporation of AI into filtering processes, which analyzes context to prevent the misclassification of legitimate educational resources. This precise, adaptive security posture minimizes false positives while maintaining robust protection, which helps ensure that technical controls support, rather than hinder, educational objections. Content Monitoring Systems (CMS), such as Gaggle Safety Management and Lightspeed Alert, fulfill the crucial cybersecurity role of

internal detection. They analyze the contents of user-generated communications and files within school-issued platforms to identify threats that have bypassed perimeter filters or originated from compromised internal accounts.

11. Content Filtering Systems (CFS) and Content Monitoring Systems (CMS) are no longer specialized compliance tools but are mandatory, high-impact security layers essential for modern K-12 cyber defense. The CFS provides proactive, perimeter-level prevention, characterized by deep SSL/TLS inspection and integration with external threat intelligence, stopping threats before they enter the network. The CMS provides crucial internal visibility and defense against lateral movement and data exfiltration, functioning as the district's primary Data Loss Prevention (DLP) mechanism within cloud environments. Their combined, integrated application forms a cohesive security fabric, delivering protection that follows the student and device regardless of location, effectively mitigating complex threats like sophisticated phishing and ransomware.

12. GCISD operates proprietary content filtering and student monitoring systems (e.g., Lightspeed and Gaggle) as essential security controls mandated by federal and state law, including CIPA. Disclosure of the operational specifics of these systems – including algorithmic logic, proprietary detection rules, and specific trigger word lists – would not merely compromise security; it would instantly and irreparably nullify the effectiveness of these protective measures. The efficacy of any preventive security control is directly dependent upon the confidentiality of its mechanism. Compelled disclosure transforms a necessary and effective security control into a known and exploitable vulnerability.

13. The request for information by the Knight Institute seeks highly sensitive operational data integral to the systems' ability to detect and prevent harm. The release of this

confidential material poses immediate, foreseeable, and catastrophic harm across multiple domains. Operationally, it allows student or external malicious actors to craft communications, documents, and network activities specifically designed to bypass detection, directly enabling prohibited activities like cyber-bullying, accessing harmful content, or coordinating violence and self-harm. Disclosure would likely result in the nullification of CIPA compliance, the exposure of GCISD's critical infrastructure, and the destruction of the third-party vendors' valuable intellectual property.

14. GCISD's affirmative duty to protect students under federal laws such CIPA requires the implementation of safety policies that prevent "hacking" and "unlawful activities." If the compelled disclosure of the system's operational logic provides a guaranteed roadmap for circumvention, this disclosure itself fundamentally renders GCISD's CIPA policy inadequate, violating the federal mandate. The security mandate, therefore, functions as a legal shield against disclosure.

15. The monitoring and filtering systems (like Lightspeed and Gaggle) are the core technological mechanisms GCISD utilizes to fulfill CIPA's mandates. If the precise logic and trigger lists are known, students can easily adjust their communication patterns to guarantee non-detection, thereby achieving "unauthorized access" to harmful content and circumventing security policies. This outcome would instantaneously render GCISD non-compliant with federal law.

16. The monitoring system's ability to proactively flag and prevent incidents of self-harm, bullying violence, and drug use is entirely dependent on the secrecy of its detection thresholds. The moment the specific algorithmic logic, scoring weights, and trigger word lists are publicized, malicious actors gain the perfect blueprint for evasion. If the system is designed to detect certain phrases associated with suicidal ideation, publishing those phrases allows a

determined student – or a peer coercing them – to craft messages or documents that successfully bypass the filter. This deliberate circumvention guarantees non-detection, resulting in the catastrophic failure of GCISD's mandate duty to intervene.

17. The information sought by the Knight Institute provides far more than just content filtering insight; it offers critical intelligence regarding GCISD's overall network architecture, security layers, and defense protocols. Knowledge of the filtering system's operational parameters and vulnerabilities allows sophisticated malicious actors – including external hackers – to execute targeted, stealthy cyberattacks. For example, by understanding the specific monitoring traps set by the Lightspeed or Gaggle systems, a hacker can design phishing emails or ransomware deployment tools that are specifically tailored to bypass those known security filters. This outcome creates a known, actionable vulnerability. It directly facilitates "unauthorized access" and "hacking," placing GCISD in direct conflict with the anti-hacking mandates of CIPA. If the disclosure provides the key to unlocking the network for data exfiltration or ransomware deployment, GCISD will have actively compromised its own network security architecture, contravening its primary obligation to safeguard student data under the Family Educational Rights and privacy Act ("FERPA").

18. Attached to this declaration as Exhibit 1 is a true and correct copy of my November 19, 2025, expert report in this lawsuit. I re-affirm the statements and opinions in my report, which are incorporated into this declaration by this reference.

19. I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED ON Dec 3rd, 2025.

Kyle Berger

EXHIBIT 1

CAUSE NO. 348-362718-25

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY,	§	**IN THE DISTRICT COURT OF**
Plaintiff,	§	
v.	§	**348TH JUDICIAL DISTRICT**
GRAPEVINE-COLLEYVILLE INDEPENDENT SCHOOL DISTRICT,	§	
Defendant.	§	**TARRANT COUNTY, TEXAS**

EXPERT REPORT OF KYLE BERGER

Kyle Berger provides the following expert report in the above-styled lawsuit.

1. Introduction

I am the Chief Technology Officer for Grapevine-Colleyville Independent School District ("GCISD"). As Chief Technology Officer my duties and responsibilities include direct the technology vision and strategy for the school district. I oversee the entire Technology Department, including network infrastructure, data management, cybersecurity, and operational support. A detailed description of my experience and qualifications is attached hereto as Exhibit 1.

I have been asked to (1) opine on whether the materials at issue in this lawsuit that were withheld from disclosure by GCISD "relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network" (see Tex. Gov't Code §552.139(a)), and (2) comment on the opinions expressed in the Expert Report of Bruce Schneier.

I am not being compensated for this report over and above my normal salary as GCISD's Chief Technology Officer.

2. Opinion

The GCISD network is founded on a dedicated, high-capacity fiber optic backbone spanning over 45 miles, which provides resilient connectivity to all 24 instructional and operational facilities across the district community. This highly dense infrastructure supports a 1:1 digital learning environment, managing in excess of 45,000 unique device connections daily for over 16,000 assigned end-users (students and staff) across both comprehensive wired and high-density wireless systems. GCISD utilizes a robust hybrid operational model, maintaining two distinct physical data center facilities integrated seamlessly with multi-tenant cloud services, all managed with a critical 24/7/365 operational commitment to ensure continuous availability.

The network is engineered to support all critical district functions, including high-bandwidth instructional services, Voice over IP (VoIP) telephony, Safety and Security systems (surveillance and access control), and administrative Enterprise Resource Planning (ERP). To protect this mission-critical environment, the network employs a defense-in-depth approach utilizing top-tier firewall systems and comprehensive cybersecurity protection tools specifically compliant with student data regulations. The overall complexity of the network is significantly elevated by its capacity to support and securely manage global virtual learning platforms, necessitating sophisticated remote access infrastructure and bandwidth optimization for a geographically distributed user base.

GCISD, as a recipient of federal funding, is subject to the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763 (2000), which was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. This legislative requirement, which must be fulfilled for GCISD to remain eligible for federal funding, forces the adoption of core technology for GCISD's computer network, including content filtering. As GCISD's Chief Technology Officer, part of my duties and responsibilities include

making sure that the design and operation of GCISD's computer network complies with CIPA – importantly, relevant to the design or operation of GCISD's computer network, ***student email accounts and internet access are part of GCISD's computer network***.

Critical to GCISD's design or operation of its computer network, GCISD is required under CIPA to have blocking or filtering measures in place to address the following: access by minors to inappropriate matter on the internet; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking," and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and measures restricting minors' access to materials harmful to them. Beyond simple blocking, CIPA further requires schools to approve and publicly adopt an internet safety policy that covers restricting access to harmful content, ensuring safe communications, preventing unlawful online activities, and protecting student data. The filtering and monitoring systems provide the necessary auditing and enforcement tools to prove that this policy is actively implemented and adhered to across all devises used by students to access the internet.

As part of its efforts to comply with CIPA, GCISD has retained the services of third-party vendors Lightspeed Solutions and Gaggle.Net to create and implement appropriate blocking and filtering measures for its computer network. GCISD has service contracts with both Gaggle.Net and Lightspeed Solutions to provide filter/monitoring systems for GCISD's computer network. These systems are used as a tool to maximize the detection of unsafe, graphic, and/or obscene student communications and website content on school district devices. With Gaggle.Net, for example, search terms that implicate computer searches that indicate suicide ideation, or self-harm and threats of violence, or obscenity will result in email notifications to GCISD and immediate

emergency phone calls if necessary. Similarly, Lightspeed Solutions monitors students' online activity on GCISD's computer network by utilizing web content filtering technology to protect students from harmful online content – in other words, Lightspeed Solutions' filter technology blocks obscene material on any devise using GCISD's computer network.[1] Notably, GCISD does ***not*** customize the lists of keywords or phrases to be monitored; rather, these lists are solely created and maintained by the district's computer service providers Lightspeed Solutions and Gaggle.Net. Both vendors consider their lists to be proprietary.

To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system.

When I say Lightspeed's filtering system "protects against malware and online threats," I mean it acts as a proactive gatekeeper that monitors, categorizes, and blocks high-risk traffic before exposure occurs. This reduces the likelihood of exploit delivery, phishing, or ransomware reaching endpoints and helps safeguard student data. How Lightspeed's filtering system helps defend K-12 (kindergarten – 12th grade) school environments against malware and cyberthreats includes:

[1] Content filtering solutions, such as Lightspeed Filter, are designed to function as the first line of defense, proactively preventing users from initiating connections with known malicious domains or downloading harmful content. Modern content filtering solutions has evolved from basic CIPA compliance tools into sophisticated security components akin to next-generation firewalls, capable of addressing the complex challenges of the contemporary threat landscape.

- The system blocks and detects attempts to access or search for known or potentially malicious websites or services, including those hidden in encrypted traffic through TLS inspection. This reduces the attack surface and improves both cybersecurity and digital safety posture.

- It integrates threat-intelligence feeds from multiple industry sources, including PhishTank, vxIntel, Internet Watch Foundation (IWF), and MI6, paired with Lightspeed's proprietary AI categorization engine to detect new and emerging threat domains and proactively block newly registered or uncategorized sites.

- It uses devise-level SmartAgents and extensions on Windows, Chrome, Mac, and iOS so filtering and threat prevention apply whether district-owned devices are on the school network or off-campus/home.

- It detects and blocks access to domain-sharing and file-hosting services frequently used to distribute malware, phishing pages, or inappropriate material, reducing risk across both cybersecurity and student-safety vectors.

- It blocks anonymizers and high-risk networks like TOR outright and continues filtering VPN traffic since enforcement occurs at the device level.

- Beyond blocking malicious sites, the monitoring and reporting of our system detects users activity, such as suspicious search terms, to identify users who are attempting to circumvent protections, evade filtering, and put compliance and security at risk.

Solutions like Lightspeed's filtering system provide end-to-end content filtering, offering critical protection against cyber risks and distractions. The system employs device-level agents to ensure comprehensive coverage across platforms such as Windows, macOS, and Chrome/Edge browsers, meaning protection follows the device regardless of whether it is on or off the campus network. This focus on coverage across all devices is functionally an evolution of the filtering system into a network-aware Endpoint Detection and Response (EDR) component, ensuring that infections acquired off-network do not compromise the district network upon reconnection. The Filter leverages specific, cybersecurity-focused categories to prevent users from accessing harmful content, including features designed to trigger immediate "internet lockouts" when malicious or harmful content is detected. This capability supports the containment phase of incident response, limiting the potential spread of malware. The accuracy of blocking is enhanced by the

incorporation of AI into filtering processes, which analyzes context to prevent the misclassification of legitimate educational resources. This precise, adaptive security posture minimizes false positives while maintaining robust protection, which helps ensure that technical controls support, rather than hinder, educational objections. Content Monitoring Systems (CMS), such as Gaggle Safety Management and Lightspeed Alert, fulfill the crucial cybersecurity role of internal detection. They analyze the contents of user-generated communications and files within school-issued platforms to identify threats that have bypassed perimeter filters or originated from compromised internal accounts.

Content Filtering Systems (CFS) and Content Monitoring Systems (CMS) are no longer specialized compliance tools but are mandatory, high-impact security layers essential for modern K-12 cyber defense. The CFS provides proactive, perimeter-level prevention, characterized by deep SSL/TLS inspection and integration with external threat intelligence, stopping threats before they enter the network. The CMS provides crucial internal visibility and defense against lateral movement and data exfiltration, functioning as the district's primary Data Loss Prevention (DLP) mechanism within cloud environments. Their combined, integrated application forms a cohesive security fabric, delivering protection that follows the student and device regardless of location, effectively mitigating complex threats like sophisticated phishing and ransomware.

GCISD operates proprietary content filtering and student monitoring systems (e.g., Lightspeed and Gaggle) as essential security controls mandated by federal and state law, including CIPA. Disclosure of the operational specifics of these systems – including algorithmic logic, proprietary detection rules, and specific trigger word lists – would not merely compromise security; it would instantly and irreparably nullify the effectiveness of these protective measures. The efficacy of any preventive security control is directly dependent upon the confidentiality of its

mechanism. Compelled disclosure transforms a necessary and effective security control into a known and exploitable vulnerability.

The request for information by the Knight Institute seeks highly sensitive operational data integral to the systems' ability to detect and prevent harm. The release of this confidential material poses immediate, foreseeable, and catastrophic harm across multiple domains. Operationally, it allows student or external malicious actors to craft communications, documents, and network activities specifically designed to bypass detection, directly enabling prohibited activities like cyber-bullying, accessing harmful content, or coordinating violence and self-harm. Disclosure would likely result in the nullification of CIPA compliance, the exposure of GCISD's critical infrastructure, and the destruction of the third-party vendors' valuable intellectual property.

GCISD's affirmative duty to protect students under federal laws such CIPA requires the implementation of safety policies that prevent "hacking" and "unlawful activities." If the compelled disclosure of the system's operational logic provides a guaranteed roadmap for circumvention, this disclosure itself fundamentally renders GCISD's CIPA policy inadequate, violating the federal mandate. The security mandate, therefore, functions as a legal shield against disclosure.

The monitoring and filtering systems (like Lightspeed and Gaggle) are the core technological mechanisms GCISD utilizes to fulfill CIPA's mandates. If the precise logic and trigger lists are known, students can easily adjust their communication patterns to guarantee non-detection, thereby achieving "unauthorized access" to harmful content and circumventing security policies. This outcome would instantaneously render GCISD non-compliant with federal law.

The monitoring system's ability to proactively flag and prevent incidents of self-harm, bullying violence, and drug use is entirely dependent on the secrecy of its detection thresholds.

The moment the specific algorithmic logic, scoring weights, and trigger word lists are publicized, malicious actors gain the perfect blueprint for evasion. If the system is designed to detect certain phrases associated with suicidal ideation, publishing those phrases allows a determined student – or a peer coercing them – to craft messages or documents that successfully bypass the filter. This deliberate circumvention guarantees non-detection, resulting in the catastrophic failure of GCISD's mandate duty to intervene.

The information sought by the Knight Institute provides far more than just content filtering insight; it offers critical intelligence regarding GCISD's overall network architecture, security layers, and defense protocols. Knowledge of the filtering system's operational parameters and vulnerabilities allows sophisticated malicious actors – including external hackers – to execute targeted, stealthy cyberattacks. For example, by understanding the specific monitoring traps set by the Lightspeed or Gaggle systems, a hacker can design phishing emails or ransomware deployment tools that are specifically tailored to bypass those known security filters. This outcome creates a known, actionable vulnerability. It directly facilitates "unauthorized access" and "hacking," placing GCISD in direct conflict with the anti-hacking mandates of CIPA. If the disclosure provides the key to unlocking the network for data exfiltration or ransomware deployment, GCISD will have actively compromised its own network security architecture, contravening its primary obligation to safeguard student data under the Family Educational Rights and privacy Act ("FERPA").

Section 552.139(a) of the Texas Government Code provides that "Information is excepted [from disclosure] if it is ***information that relates to*** computer network security, to restricted information under Section 2059.005, or to ***the design, operation, or defense of a computer network.***"

I have been informed by counsel that the courts have held that the phrase "relates to," as used in other sections of the Public Information Act, "is ***very broad***, encompassing even information that would not be 'relevant,' in the evidentiary sense, during litigation." *B.W.B. v. Eanes Indep. Sch. Dist.*, 2018 Tex. App. Lexis 223, *19 (Tex. App. – Austin 2018, no pet.) (emphasis added); see also *City of San Antonio v. Abbott*, 432 S.W.3d 429, 432 (Tex. App. – Austin 2014, pet. denied) ("The plain meaning of the phrase 'relates to' is 'to have a connection with, to refer to, or to concern.' In ordinary use, the phrase 'relates to' is ***very broad.***") (emphasis added).

To summarize, GCISD has "designed" and is "operating" its computer network by using/installing/incorporating the Gaggle.Net and Lightspeed Solutions filtering systems into the school district's computer network. Thus, interpreting the term "relates to" as used in Government Code §552.139(a) ***"very broadly,"*** the word lists and analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's computer network and, therefore, should be excepted from disclosure to the Knight Institute pursuant to Tex. Gov't Code §552.139(a).

3. Response to Schneier Report

I first note that Mr. Schneier's report only addresses whether the disclosure of the information requested by the Knight Institute would increase the risk of a threat to GCISD's "computer network security." His report fails, however, to address whether the requested information "relates to" "the design, operation or defense of [GCISD's] computer network." See Tex. Gov't Code § 552.139 (excepting from disclosure information that "relates to" either "network security" or[2] "the design, operation or defense of a computer network"). As stated above,

[2] The word "or" as used in the Government Code is defined in the dictionary as "used as a function word to indicate an alternative." See *Webster's New Collegiate Dictionary* (1981) p. 800.

it is my opinion that the requested information *does* "relate to" the "the design, operation or defense of GCISD's computer network."

Next, I firmly reject Mr. Schneier's conclusion that disclosing the mechanisms used to monitor and trigger alerts would pose no threat to GCISD's computer network security. This conclusion relies on an overly narrow, traditional industry definition of "computer network security" that fails to account for the unique, mandatory, and integrated statutory duties placed on K-12 institutions regarding student safety and critical infrastructure protection.

Mr. Schneier, defines "computer network security" in the cybersecurity industry as defenses against unauthorized access by external actors, focusing on threats like cyberattacks, malware, and ransomware. He explicitly states that network security measures are not used to refer to defenses against unauthorized use by someone who already has authorized access.

Based on this distinction, Mr. Schneier concludes that releasing the requested information – the specific blocked websites and monitored keywords – concerns "impedes uses of its devices by authorized users" (students). Therefore, disclosing this information would not increase the likelihood of a computer security incident because it would not facilitate unauthorized access by external actors or lead to the harm or destruction of digital devices.

I counter this argument by asserting that in the K-12 environment, student safety monitoring (Content Monitoring Systems, or CMS) and network security (Content Filtering Systems, or CFS) have a strategic convergence, and compromising one fatally compromises the other, resulting in the "catastrophic failure" of mandated federal duties.

The key vulnerability created by disclosure is not merely allowing "unauthorized use" by enabling circumvention, which GCISD's duties explicitly prohibit. For example,

- Guaranteed Roadmap for Evasion: The requested information includes proprietary trigger word lists, specific algorithmic weights, and confidential machine learning model parameters. Disclosure of this core proprietary logic would provide a guaranteed roadmap for circumvention, resulting in non-detection.
- Circumvention Equates to Unauthorized Activity: CIPA mandates that GCISD must implement safety policies addressing "unauthorized access, including so-called 'hacking,' and other unlawful activities by minors online". If the precise detection logic and trigger lists are known, students can easily adjust their communication patterns to guarantee non-detection, thereby achieving "unauthorized access" to harmful content and circumventing security policies. This outcome instantly renders GCISD non-compliant with the federal anti-hacking mandate.
- Facilitating External Cyberattacks: The expert's view focuses solely on external intrusion. However, the defense brief argues that knowledge of the filter and monitoring system's operational parameters and vulnerabilities allows sophisticated malicious actors (external hackers) to execute targeted, stealthy cyberattacks. A hacker could design phishing emails or ransomware deployment tools specifically tailored to bypass those known security filters, which directly facilitates "unauthorized access" and "hacking". The system's ability to flag a student researching security bypass methods is simultaneously generating a critical Indicator of Compromise (IOC).
- Critical Infrastructure Information (CII): GCISD's network infrastructure, which holds massive amounts of PII for minors and serves as the primary early warning system for preventing imminent violence/self-harm, must be legally recognized as

> Critical Infrastructure (CII). This status warrants protection under public records law exemptions that shield "detection mechanisms or security configurations". Publishing detection logic creates a systemic vulnerability comparable to publishing the blueprints or a power grid's security systems.

In conclusion, GCISD's use of Lightspeed and Gaggle is a layered security approach integrating proactive prevention (CFS) and internal detection (CMS). To separate the "security" function (external hacking prevention) from the "safety" function (internal threat detection) is to ignore the reality that these systems converge operationally and rely on the same proprietary detection logic. Disclosure would transform GCISD's security controls into a known, actionable vulnerability, directly contravening its non-delegable statutory duties to protect students and secure its digital environment.

4. Conclusion

To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system.[3]

[3] In addition to CIPA compliance, Lightspeed Solutions' filtering system also assists GCISD with complying with other student internet safety regulations such as Texas Senate Bill 1893 (effective September 1, 2023), which "prohibit[s] the use of certain social media applications and services on devices owned or leased by governmental entities."

To summarize, GCISD has "designed" and is "operating" its computer network by using/installing/incorporating the Gaggle.Net and Lightspeed Solutions filtering systems into the school district's computer network. Thus, interpreting the term "relates to" as used in Government Code §552.139(a) ***"very broadly,"*** the word lists and analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's computer network and, therefore, should be excepted from disclosure to the Knight Institute pursuant to Tex. Gov't Code §552.139(a).

Date: November 19, 2025.

Kyle Berger