

CAUSE NO. \_\_\_\_\_

THE STATE OF TEXAS

*Plaintiff,*

v.

POWERSCHOOL HOLDINGS, INC.,  
POWERSCHOOL GROUP, LLC.

*Defendant.*

§  
§  
§  
§  
§  
§  
§  
§

IN THE DISTRICT COURT

COLLIN COUNTY, TEXAS

\_\_\_\_\_ JUDICIAL DISTRICT

**PLAINTIFF’S ORIGINAL PETITION**

Defendants PowerSchool Holdings, Inc. and PowerSchool Group, LLC (collectively “PowerSchool”) fail to protect sensitive personal information belonging to Texas school-aged children and teachers. For years, PowerSchool has misrepresented the nature and extent of its data privacy and security protections to Texas schools who entrust PowerSchool with their students’ and teachers’ highly sensitive personal information, including social security numbers and protected health information. In December of 2024, these failures resulted in a catastrophic data breach impacting over 800,000 Texas students and teachers. The State of Texas, acting by and through the Attorney General of Texas, Ken Paxton, brings this action in the public interest to stop PowerSchool’s deceptive trade practices and hold them accountable for their data privacy and security failures.

**DEFENDANTS**

1. Defendant PowerSchool Holdings, Inc., is a Delaware corporation with its principal place of business at 150 Parkshore Drive, Folsom, California 95630. Defendant PowerSchool Holdings, Inc., may be served through its registered agent The Corporation Trust Company at the following address: 1209 Orange St., Wilmington, DE 19801.

2. Defendant PowerSchool Group LLC is a Delaware Limited Liability Company with its principal place of business at 150 Parkshore Drive, Folsom, California 95630. Defendant PowerSchool Group LLC may be served through its registered agent United Corporate Services, Inc. at the following address: 815 Bravos St., Suite 500, Austin, TX 78701.

### **JURISDICTION AND VENUE**

3. Venue for this action properly lies in Collin County, Texas, because: 1) a substantial part of the events or omissions giving rise to the State of Texas's claims occurred in Collin County; 2) transactions made part of this suit occurred in Collin County; 3) PowerSchool has done business in Collin County; 4) PowerSchool has engaged in trade and commerce in Collin County; and 5) victims of PowerSchool's unauthorized disclosure of personal and sensitive information reside in Collin County. *See* Tex. Civ. Prac. & Rem. Code § 15.002(a)(1), Tex. Bus. & Com. Code § 17.47(b), and Tex. Bus. & Com. Code § 521.151(c)(2).

4. The Court has general jurisdiction over PowerSchool because their contacts and affiliations with Texas are so continuous and systematic as to render them essentially at home in Texas. *Luciano v. SprayFoamPolymers.com, LLC*, 625 S.W.3d 1, 8 (Tex. 2021) (citing *TV Azteca v. Ruiz*, 490 S.W.3d 29, 37 (Tex. 2016)).

5. Alternatively, the Court has specific jurisdiction over PowerSchool because they purposefully availed themselves of the privileges of conducting activities in Texas, specifically targeted the Texas market, and the causes of action in this suit arise out of or relate to PowerSchool's contacts in Texas. *See BRP-Rotax GmbH & Co. KG v. Shaik*, No. 23-0756, 2025 WL 1727903 at \*8 (Tex. 2025).

## **DISCOVERY**

6. Discovery in this case should be conducted under Level 3, pursuant to Tex. R. Civ. P. 190.4.

7. This case is not subject to the restrictions of expedited discovery under Tex. R. Civ. P. 169, because Texas seeks nonmonetary injunctive relief.

8. Texas claims entitlement to monetary relief in an amount greater than \$1,000,000 including civil penalties, reasonable attorneys' fees, litigation expenses, investigation expenses, and costs.

## **THE DECEPTIVE TRADE PRACTICES ACT (DTPA)**

9. The Texas Deceptive Trade Practices Act ("DTPA") declares unlawful any "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce." Tex. Bus. & Com. Code § 17.46(a). This includes "representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not," Tex. Bus. & Com. Code § 17.46(b)(5), "representing that goods or services are of a particular, standard, quality, or grade, or that goods are of a particular style or model, if they are of another," Tex. Bus. & Com. Code § 17.46(b)(7), and "failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed," Tex. Bus. & Com. Code § 17.46(b)(24).

10. Under the DTPA, "an act is false, misleading, or deceptive if it has the capacity to deceive an ignorant, unthinking, or credulous person." *Doe v. Boys Clubs of Greater Dallas, Inc.*,

907 S.W.2d 472, 479–80 (Tex. 1995) (*quoting Spradling v. Williams*, 566 S.W.2d 561, 562 (Tex. 1978)); *see also Streber v. Hunter*, 221 F.3d 701, 728 (5th Cir. 2000) (same).

11. Tex. Bus. & Com. Code § 17.45(6) defines “trade” and “commerce” as “the advertising, offering for sale, sale, lease, or distribution of any good or service, of any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value, wherever situated, and shall include any trade or commerce directly or indirectly affecting the people of this state.”

12. Tex. Bus. & Com. Code § 17.45(2) defines “services” as “work, labor, or service purchased or leased for use, including services furnished in connection with the sale or repair of goods.” *See also Riverside Nat’l Bank v. Lewis*, 603 S.W.2d 169, 174 (Tex. 1980) (“services” means “action or use that furthers some end or purpose: conduct or performance that assists or benefits someone or something: deeds useful or instrumental toward some object.”).

13. The DTPA mandates that the law “*shall be liberally construed* and applied to promote its underlying purposes, which are to protect consumers against false, misleading, and deceptive business practices, unconscionable actions, and breaches of warranty and to provide efficient and economical procedures to secure such protection.” Tex. Bus. & Com. Code § 17.44(a) (emphasis added); *see also Singleton v. Pennington*, 568 S.W.2d 382, 385 (Tex. Civ. App.—Dallas 1978).

14. The DTPA provides a cause of action for deceptive trade practices “without the burden of proof and numerous defenses encountered in a common law suit.” *Sergeant Oil & Gas Co., Inc. v. Nat’l Maint. & Repair, Inc.*, 861 F. Supp. 1351, 1365 (S.D. Tex. 1994).

## IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

15. The Identity Theft Enforcement and Protection Act (“ITEPA”) requires that “[a] business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.” Tex. Bus. & Com. Code § 521.052(a); *see also Texas Comptroller of Pub. Accounts v. Atty. Gen. of Texas*, 354 S.W.3d 336, 355 (Tex. 2010) (Wainright, J. and Johnson, J., dissenting in-part and concurring in-part) (“the Texas Identity Theft Enforcement and Protection Act requires businesses to take reasonable steps to protect “sensitive personal information” collected or maintained by the business in the regular course.”).

16. Section 521.002 of ITEPA defines “Personal identifying information” as “information that alone or in conjunction with other information identifies an individual, including an individual’s:

- (A) name, social security number, date of birth, or government-issued identification number;
- (B) mother’s maiden name;
- (C) unique biometric data, including the individual’s fingerprint, voice print, and retina or iris image;
- (D) unique electronic identification number, address, or routing code; and
- (E) telecommunication access device as defined by Section 32.51, Penal Code.

17. Further, Section 521.002 of ITEPA defines “Sensitive personal information” as follows:

- (A) an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - (i) social security number;
  - (ii) driver’s license number or government-issued identification number;or

- (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- (B) information that identifies an individual and relates to:
  - (i) the physical or mental health or condition of the individual;
  - (ii) the provision of health care to the individual; or
  - (iii) payment for the provision of health care to the individual.

### **PUBLIC INTEREST**

18. The Consumer Protection Division has reason to believe that PowerSchool is engaging in, has engaged in, or is about to engage in an act or practice declared to be unlawful under the DTPA and that proceedings would be in the public interest to restrain by permanent injunction the use of such method, act, or practice. Tex. Bus. & Com. Code § 17.47(a).

### **FACTS**

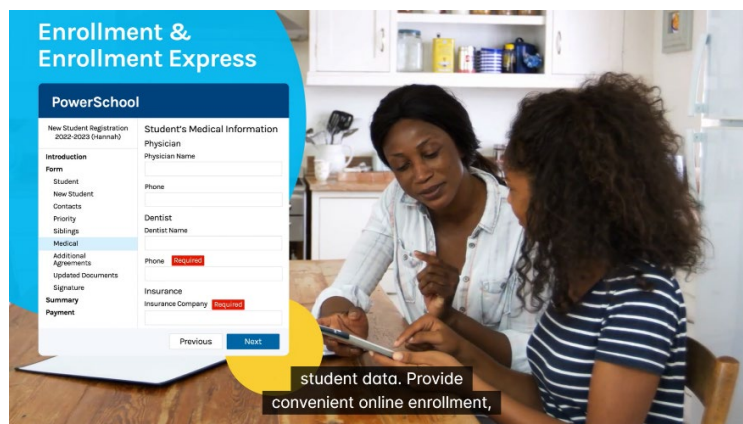
19. PowerSchool provides education technology software services to K-12 schools throughout the United States. PowerSchool's software collects, maintains, and is responsible for processing and securing the sensitive information that Texas schools require parents to provide to enroll their children in education. *See PowerSchool Enrollment*, PowerSchool, <https://www.powerschool.com/solutions/student-information/enrollment/> (last visited Aug. 25, 2025) ("Powering registration for millions of students across thousands of districts."); *see* Tex. Educ. Code. § 25.085.

20. PowerSchool's software also collects, maintains, and is responsible for processing and securing the sensitive information that Texas schools require from their employees in order to meet administrative and operational needs such as payroll, compliance reporting, and management. *See PowerSchool Employee Records*, PowerSchool,

<https://www.powerschool.com/solutions/talent-recruitment-retention/employee-records/> (last visited Aug. 25, 2025).

21. Besides the hundreds of millions of dollars that Texas taxpayers spend on PowerSchool's contracts with Texas schools, PowerSchool also benefits financially from commercial uses of school-aged children's data. PowerSchool uses school-aged children's data to develop its products and sell it to third parties. Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, The Markup (Jan. 14, 2022 at 17:14 ET), <https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students> (Naviance, a PowerSchool owned product, "gathers data through its college guidance software and then allows colleges and universities to target students with paid advertisements encouraging them to enroll.").

22. PowerSchool School Information System ("Powerschool SIS") is a "core data management system" that Texas schools use to manage the personal identifiable information ("PII"), sensitive identifiable information ("SPI"), and protected health information ("PHI") that schools receive regarding Texas school-aged children and teachers. Through PowerSchool SIS, PowerSchool is responsible for collecting, storing, and maintaining PII, SPI, and PHI.



*Figure 1: “Student Medical Information” form in a PowerSchool SIS advertisement.*

23. PowerSchool has described PowerSchool SIS as “the mission-critical data backbone that powers K-12 operations” and stated that it “serves as the hub and single source of truth for student data.” PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 11 (Mar. 24, 2022).

24. PowerSchool collects and stores PII, SPI, PHI, and other highly sensitive information belonging to all of its Texas school-aged children and their teachers in two unencrypted databases. The databases include data such as:

- a. Names, dates of birth, and home address;
- b. Social Security numbers;
- c. Disability information;
- d. Attendance records;
- e. Grades;
- f. Medical information, such as physician names; and
- g. Bus stops.

Ex. A PowerSchool SIS Data Dictionary, Students(ver3.6.1), *PowerSchool*; Ex. B PowerSchool SIS Data Dictionary, Teachers (ver7.8.0), *PowerSchool*.

25. PowerSchool also owns and operates PowerSource, a customer support platform that allows third-party support vendors to access PowerSchool’s systems for maintenance and support purposes. *Terms of Use*, PowerSource, <https://support.powerschool.com/tos.action> (last visited Aug. 25, 2025).

26. PowerSchool has experienced vast success in the education technology industry by collecting, storing, and analyzing data belonging to school-aged children and teachers. Once a

publicly traded company, PowerSchool went private after being acquired by Bain Capital for \$5.6 billion in 2024. *Bain Capital Completes Acquisition of PowerSchool*, PowerSchool, <https://www.powerschool.com/bain-capital/> (last visited August 21, 2025).

## **I. PowerSchool’s False and Misleading Privacy and Security Representations**

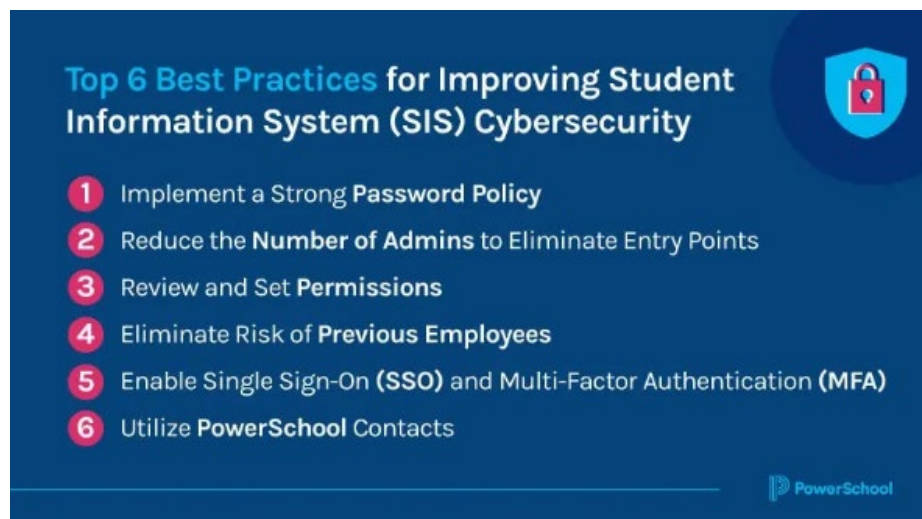
27. PowerSchool falsely and misleadingly represents the extent to which it maintains and protects the privacy, security, confidentiality, or integrity of PII, SPI, and PHI belonging to school-aged children and teachers, in violation of the DTPA.

28. For years, PowerSchool’s webpage misleadingly advertised PowerSchool’s “commit[ment] to being a good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability.” *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, <https://www.powerschool.com/security/> [<https://web.archive.org/web/20241208221923/https://www.powerschool.com/security/>].

29. In August of 2023, the Biden-Harris administration invited PowerSchool to speak at Jill Biden’s *Back to School Safely: K-12 Cybersecurity and Data Protection Initiative*. There, PowerSchool’s CEO Hardeep Gulati used the Biden White House’s podium to deceptively boast of its “relentless investment and focus on every element of security.” *POWERSCHOOL, Hardeep Gulati at Dr. Jill Biden’s Back to School Safely: Cybersecurity Summit for K12 Schools Event*, at 2:20 (YouTube, Aug. 8, 2023), <https://www.youtube.com/watch?v=sS41XlZQe7U>. In PowerSchool’s blog linked to this video about Biden’s event, PowerSchool re-iterated it was “taking all reasonable and appropriate countermeasures to protect students’ and teachers’ data.” Hardeep Gulati, *PowerSchool Presents Cybersecurity Commitments at White House K-12 Cybersecurity & Data Privacy Event*, PowerSchool (Sep. 21, 2023),

<https://www.powerschool.com/blog/powerschool-presents-cybersecurity-commitments-at-white-house-k-12-cybersecurity-data-privacy-event/>.

30. On September 10, 2024, a PowerSchool blog recommended that its customers improve security by reducing the amount of administrative access privileges they grant and utilizing single sign-on (SSO) and Multi-Factor Authentication (MFA). *Top 6 Best Practices for Improving Student Information System (SIS) Cybersecurity* | PowerSchool, PowerSchool, <https://www.powerschool.com/blog/best-practices-improving-sis-cybersecurity/> (last visited Aug. 21, 2025). It included the following “Top 6 Best Practices” infographic:



*Id.*

31. On June 20, 2023, PowerSchool published a blog listing the eight “best practices” for student data privacy. *Student Data Privacy: Everything You Need to Know*, PowerSchool, <https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/> (last visited Aug. 21, 2025). Practice four, titled “Secure Data Storage and Sharing,” advises schools to “[r]estrict data access to only those users who have to have it and implement strong authentication protocols.” *Id.* The blog further describes “How PowerSchool Provides Superior Student Data

Privacy and Security,” by listing privacy and security practices including achieving the International Standards Organization 27000 series certification and ensuring data residency “with no information going offshore.” *Id.*

32. For years, PowerSchool represented that it employed a “variety of physical, administrative, and technological safeguards designed to protect... data against loss, misuse, and unauthorized access or disclosure” and that it “consider[ed] the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data.” *Global Privacy Statement*, PowerSchool, <https://www.powerschool.com/privacy/> [<https://web.archive.org/web/20241004033859/https://www.powerschool.com/privacy/>].

33. Through the same webpage, PowerSchool stated that it “keep[s] information collected on behalf of [PowerSchool’s] Customers for as long as necessary to fulfill the purpose for which it was collected, pursuant to contractual terms or as otherwise required by applicable law” and that PowerSchool “dispose[s] of information that is not held pursuant to contractual terms within a commercially reasonable period or at the request of a customer using reasonable measures to protect against unauthorized access to or use of information.” *Id.*

34. PowerSchool further represents that it “complies with privacy laws of the United States with respect to personal information and especially student educational records” and does “not use Student Data for any purpose other than to provide the services, in accordance with [its] contractual agreements with [its] Customers, [its] Terms of Service, and [its] Privacy Policy.” *Id.*

35. Furthermore, PowerSchool advertises that it signed the national Student Privacy Pledge. PowerSchool describes the pledge stating, “*School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security.*” *Student Data Privacy: Everything You Need to Know*, PowerSchool, *supra*.

36. PowerSchool’s Global Privacy Statement webpage includes a list titled “Frequently Asked Questions.” *Global Privacy Statement*, PowerSchool <https://www.powerschool.com/privacy/> (last visited Sept. 2, 2025). In response to the question “How does PowerSchool protect my Personal Data?”, PowerSchool answers that it “*use[s] state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that [it] process[es].*” *Id.*

37. PowerSchool has also made false and misleading statements related to a “Security by Design roadmap.” PowerSchool falsely represented that it was drafting a Security by Design roadmap to be published. *PowerSchool Presents Cybersecurity Commitments at White House K-12 Cybersecurity & Data Privacy Event*, PowerSchool (Sep. 21, 2023), *supra*. As of September 2025, PowerSchool has not published a Security by Design roadmap. As described by the Cybersecurity & Infrastructure Security Agency (“CISA”), a secure by design roadmap would “document changes made to [a software’s development lifecycle] to improve customer security” and is published “[i]n the spirit of showing rather than telling” in order to “build confidence that the products are secure by design.” *See e.g.*, Cybersecurity and Infrastructure Security Agency, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure By Design Software*, (April 13, 2023), [https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign\\_1025\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf). CISA also claims that “only by incorporating secure by design practices will we break the vicious cycle of constantly creating and applying fixes.” *Id.*

38. In addition to its public statements, PowerSchool also made false and misleading representations in its Data Privacy Agreements with schools. PowerSchool represents that it implements the following safeguards and practices, consistent with widely accepted industry standards such as NIST and ISO 27001:2022, which require:

- a. server authentication and encryption of data-at-rest and data-in-transit;
- b. identity management and authentication and access control through issuance, verification, management, auditing, and revocation as applicable of credentials and identities for authorized devices, processes, and users;
- c. employee training;
- d. monitoring of critical systems through logging and analyzing events; and
- e. management of remote access.

39. In its Texas Standard Student Data Privacy Agreement, PowerSchool represents that it will “comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.” In this agreement, PowerSchool also acknowledged and agreed to have a written incident response plan reflecting best practices and consistency with federal and state law. Ex. C Texas Standard Student Data Privacy Agreement.

40. PowerSchool acknowledges that school districts are aware of its information security representations and consider them when selecting vendors. PowerSchool states:

*In the pursuit of cybersecurity enhancement, under-resourced schools must assess the security practices of technology vendors. Prioritizing vendors with recognized certifications such as SOC 2 or ISO 27001, becomes paramount. These certifications validate a vendor’s commitment to rigorous security standards, ensuring that the integration of technology solutions doesn’t compromise data integrity. By proactively selecting vendors such as PowerSchool with established credentials in cybersecurity, schools can bolster their defenses and establish a secure digital infrastructure for sustained educational success.*

*PowerSchool Information Security Report*, PowerSchool, [https://go.powerschool.com/rs/861-RMI-846/images/Cybersecurity-Report.pdf?version=2&utm\\_medium=social/?wtime](https://go.powerschool.com/rs/861-RMI-846/images/Cybersecurity-Report.pdf?version=2&utm_medium=social/?wtime) (last visited Sep. 2, 2025). Here, the State agrees with PowerSchool. Texas schools *do* prioritize education technology vendors who make representations and commitments to rigorous security

standards, and vendors who make representations regarding their software's ability to not compromise the integrity of the personal and sensitive data that Texas school districts collect, use, and store for their students and teachers.

41. In sum, PowerSchool has a long history of consistently painting itself broadly as a company with commendable information security, and making detailed statements as to its specific information security practices that Texas school districts and students understandably rely on in making the important decision to entrust it with Texas children's and teachers' most sensitive data.

## **II. PowerSchool's Deficient Privacy Practices and Data Breach**

42. Despite these express and implicit representations, PowerSchool failed to maintain and protect the privacy, security, confidentiality, or integrity of Texas school-aged children's and teachers' data for years, directly leading to a data breach effecting over 880,000 Texas school-aged children and teachers.

43. PowerSchool's deficient privacy and security acts or practices include the following:

- a. Failure to encrypt PII, SPI, and PHI at a database level;
- b. Failure to encrypt PII, SPI, and PHI at a line level;
- c. Failure to implement adequate access limitations;
- d. Lack of multi-factor authentication ("MFA"), single sign-on ("SSO"), and other access controls for employees and contractors;
- e. Providing access to PowerSchool data through PowerSource without adequate segmentation or isolation;
- f. Inadequate data retention policies retaining unnecessary PII, SPI, and PHI;
- g. Failure to adequately monitor network traffic and credential usage;

- h. Failure to implement anomaly detection like requiring additional verification for new devices or strange IP addresses;
- i. Failure to adequately require, implement, maintain, or update anti-malware software for all employees and contractors; and
- j. Failure to adequately audit, penetration test, and evaluate the adequacy of its privacy and security acts or practices.

44. PowerSchool's failures and deficiencies led to a data breach in September 2024, in which Matthew Lane, *a teenager*, accessed PII, SPI, and PHI belonging to millions of school-aged children and parents. According to PowerSchool's May 22, 2025, Data Breach report, the breach resulted in the theft of over 881,249 Texas school-aged children's and teachers sensitive personal information. Ex. D Data Breach ID BR-0004310, *PowerSchool*.

45. To perform the breach, Lane simply used stolen login credentials belonging to one of PowerSchool's third-party contractors. The third-party contractor had administrative access to all of PowerSchool's most prized data, ignoring information security practices preached by PowerSchool like limiting access privileges. Carly Page, *Hacker accessed PowerSchool's network months before massive December breach*, TechCrunch, (Mar. 10, 2025 at 9:52 AM PDT), <https://techcrunch.com/2025/03/10/hacker-accessed-powerschools-network-months-before-massive-december-breach/>.

46. Over the course of several months Lane went on to rent a computer server from a cloud storage provider located in Ukraine and use it in combination with the previously utilized and compromised PowerSource credentials to re-access PowerSchool's systems months later from December 19, 2024, through December 23, 2024. During this period, the teenager accessed, explored, prepared, and ultimately exfiltrated two crucial .CSV files in PowerSchool SIS's system

without detection even though the access from Ukraine would have set off alerts in more reasonably protected systems. Lawrence Abrams, *PowerSchool hacker claims they stole data of 62 million students*, BLEEPING COMPUTER, (January 22, 2025), <https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/>; see, Information, *US v. Matthew Lane*, Docket No. 4:25-cr-40015-MRG (D. Mass filed May 20, 2025).

47. The two files had 150 unique data fields for more than 60 million students and 10 million teachers, countless of which are Texans. The following data was disclosed:

- a. Names, addresses, phone numbers, and emails;
- b. Social Security Numbers;
- c. Dates of Birth;
- d. Medical information, e.g. allergies and physician information;
- e. Grades and grade-point-averages;
- f. Bus Stops, which can be used to physically locate Texas children;
- g. Employment information; and
- h. Disability information.

48. Due to PowerSchool's deficient security practices, the breach was only discovered when the hacker contacted PowerSchool to demand a ransom for the deletion of the data. Kevin Collier, *Children's data hacked after school software firm missed basic security step, internal report says*, NBC News (Jan. 31, 2025, 4:00 CST), <https://www.nbcnews.com/tech/security/powerschool-hack-data-breach-protect-student-school-teacher-safe-rcna189029>.

### **III. PowerSchool’s Conduct Warrants the Maximum Imposition of Civil Penalties for Each Violation of the DTPA**

49. Under Texas Bus. & Com Code § 17.47(g), there are six factors the trier of fact “shall consider” when determining the amount of civil penalties to impose for each violation of the DTPA, which includes the following:

- (1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of any prohibited act or practice;
- (2) the history of previous violations;
- (3) the amount necessary to deter future violations;
- (4) the economic effect on the person whom the penalty is to be assessed;
- (5) Knowledge of the illegality of the act or practice; and
- (6) any other matter that justice may require.

50. The State of Texas is entitled to recover up to \$10,000 for each violation of the DTPA. Tex. Bus. & Com. Code § 17.47(c)(1).

51. To determine what amount on the spectrum of civil penalties to impose for each violation of the DTPA, the trier of fact must rely on the statute, not the extent or existence of damages suffered by any individuals. *See* Under Texas Bus. & Com Code § 17.47(g); *see also* *Avila v. State*, 252 S.W.3d 632, 637-38 (Tex. App.-Tyler 2008) (“the legislature could have included results of the defendant’s actions in the list had it so chosen... [t]estimony about the results of [defendant’s] actions is irrelevant under the DTPA”).

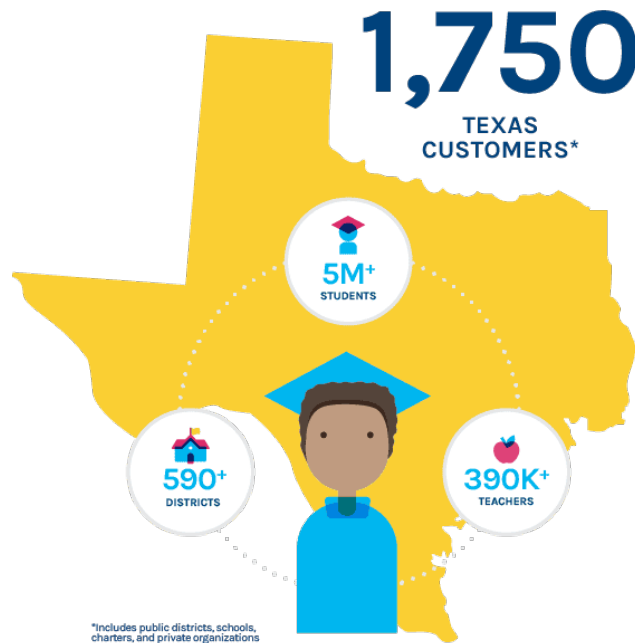
52. A defendant’s current financial situation must also be considered by the jury when determining civil penalties to impose for each violation of the DTPA. *See* Tex. Bus. & Com. Code § 17.47(g)(3)-(4), (6).

#### **A. The Seriousness of the Circumstances of PowerSchool’s Privacy and Security Practices**

53. Identity theft against children is particularly problematic because illicit use of their identity can go unnoticed, as nonprofit credit advocates describe: “[f]or children, the emotional

impact is much greater.... [i]t can take years to get wind of a problem, and meanwhile the damage can continue to grow.” Further, “[i]dentity theft against children — especially very young ones — often slips under the radar until they are older teens or young adults applying for their first credit card, trying to finance a car, or seeking student loans.” See Cheryl Winokur Munk, *Why parents may want to start locking a child’s credit at a very young age*, CNBC (Aug. 23, 2024) <https://www.cnbc.com/2024/08/23/identity-theft-of-americas-youngest-generation-is-on-the-rise.html>.

54. As the Federal Trade Commission has stated, “many school forms require personal and sensitive information.” See, e.g., Colleen Tressler, *Back to school: Protect your child’s information*, Federal Trade Commission Consumer Advice (August 20, 2018), <https://consumer.ftc.gov/consumer-alerts/2018/08/back-school-protect-your-childs-information>. The State has reason to believe that numerous Independent School Districts in Texas use PowerSchool’s SIS software to store PII, PHI, and other SPI, including but not limited to Dallas, Frisco, Plano, McKinney, Houston, Katy, Lovejoy, and more.



*Figure 2: PowerSchool graphic of its Texas operations in May 2022.*

*B. PowerSchool's Significant Control Over Texans*

56. PowerSchool exercised significant control over Texas students and teachers in districts that used PowerSchool. On information and belief, while PowerSchool grew its user base, gained influence, and benefited from its contracts with Texas school districts, Texas students and teachers had to provide the company with personal information and trust that PowerSchool would keep that information safe. Instead, PowerSchool reaped the benefits of Texans' data while failing to implement sufficient privacy and security practices.

*C. PowerSchool's Financial Success from School-Aged Children's Data*

56. PowerSchool dominates the education technology market. PowerSchool boasts its use by 90 of the top 100 school districts in the country. *PowerSchool Recognized as one of America's Fastest-Growing Private Companies on Inc. Magazine's Annual Inc. 5000 List*, PowerSchool, <https://www.powerschool.com/news/powerschool-recognized-as-one-of-americas->

fastest-growing-private-companies-on-inc-magazines-annual-inc-5000-

list/#:~:text=With%20a%20three%2Dyear%20revenue,companies%20on%20the%202020%20li  
st (last visited Sep. 2, 2025).

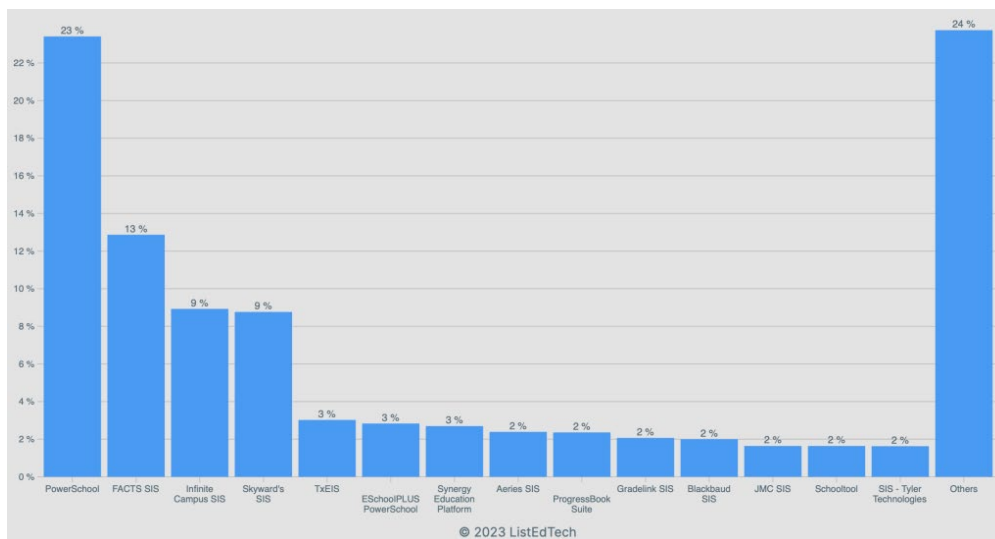


Figure 3: Ed. Tech SIS Marketshare.

Justin Ménard, *An Update On The K-12 SIS Historical Implementations*, listedtech (Oct. 24, 2023), <https://listedtech.com/blog/update-k12-student-information-system/>.

57. PowerSchool is in this enviable position because over the past decade, it has purchased its way into it. PowerSchool routinely acquires competitors, with at least 18 different acquisitions of education technology software companies since 2015. PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 11 (Feb. 29, 2024). PowerSchool admits its acquisition strategy is “core to [its] strategy” and that PowerSchool “intend[s] to continue pursuing targeted acquisitions...”. *Id.*

58. Those acquisitions include companies such as InfoSnap, the “leading provider of cloud-based registration management solutions.” *PowerSchool Acquires InfoSnap to Deliver SIS industry’s First Full-featured Online Registration Solution*, PowerSchool,

<https://www.powerschool.com/news/powerschool-acquires-infosnap-deliver-sis-industrys-first-full-featured-online-registration-solution/> (last visited Sep. 2, 2025). Similar to PowerSchool SIS, InfoSnap included services such as online application, admissions, school choice/lottery, new student enrollment, annual student registration, and staff registration.” *Id.* InfoSnap had over 10,000 customers, including Grand Prairie ISD and Keller ISD.

59. During 2020 and 2021, PowerSchool spent \$400 million acquiring education technology companies to further its market dominance. PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 104 (Mar. 24, 2022). First, PowerSchool purchased Hoonuit, a leading data analytics service, for \$81.1 million in October of 2020. *Id.* Less than five months later, PowerSchool acquired Hobsons, Inc. for \$318.9 million. *Id.* Hobsons, Inc. was a software solutions corporation consisting of Naviance and Intersect, two college preparedness software platforms. *Id.*

60. As another example, PowerSchool recently acquired SchoolMessenger in 2023 for \$300.3 million. PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 105 (Feb. 29, 2024). SchoolMessenger provided communication software services to over 63,000 schools, such as those in Kingsville ISD. *School Messenger Program for Parents & Guardians*, Kingsville ISD, [https://www.kingsvilleisd.com/apps/pages/index.jsp?uREC\\_ID=252823&type=d&pREC\\_ID=2117192](https://www.kingsvilleisd.com/apps/pages/index.jsp?uREC_ID=252823&type=d&pREC_ID=2117192) (last visited Aug. 26, 2025); see also *PowerSchool Completes Acquisition of SchoolMessenger*, PowerSchool, <https://www.powerschool.com/schoolmessenger/> (last visited Aug. 26, 2025). After the acquisition, PowerSchool “embedded [SchoolMessenger] directly into PowerSchool SIS,” for the alleged benefit to Texas Schools of the ability to “increase security and minimize risks with tightly connected systems.” *PowerSchool Completes Acquisition of SchoolMessenger*, PowerSchool, *supra*.

*C. PowerSchool Foresaw the December 2024 Breach and its Consequences*

61. While PowerSchool’s false representations misled and deceived Texas schools regarding its privacy and security practices, it was aware of the risks its deficient practices imposed on Texas Schools, their teachers, and school-aged children.

62. PowerSchool’s 2022 and 2023 Form 10-K Annual Reports relate “Risk Factors” which PowerSchool says “describe[s] circumstances that may materially harm our future business.” PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 22 (Mar. 24, 2022); PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 22 (Feb. 29, 2024). The risk factors include “the impact of potential information technology or data security breaches or other cyber-attacks or other disruptions;” “our ability to comply with privacy laws and regulations,” “our ability to comply with legal requirements, contractual obligations, and industry standards relating to security, data protection, and privacy,” “the fact that our activities are and will continue to be subject to extensive government regulation,” and “risk related to future regulation.” PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 22-23 (Mar. 24, 2022); PowerSchool Holdings, Inc., Annual Report (Form 10-K) at 22-23 (Feb. 29, 2024).

63. PowerSchool’s marketing materials also forewarned of an “84% increase in education cyberattacks from 2022-2023” and described ransomware as an “evolving threat.” *AI and K-12 Data: The Responsible Approach*, PowerSchool, [https://www.powerschool.com/wp-content/uploads/2024/03/Bringing\\_AI\\_to\\_Your\\_Data\\_Infographic.pdf](https://www.powerschool.com/wp-content/uploads/2024/03/Bringing_AI_to_Your_Data_Infographic.pdf) (last visited, Sept. 3, 2025). PowerSchool’s Annual Report in 2022 listed “risk factors” including “the impact of potential information technology or data security breaches or other cyber-attacks.” *AI and K-12 Data: The Responsible Approach*, PowerSchool, <https://www.powerschool.com/infographic/ai-and-k-12-data-the-responsible-approach/> (last visited Aug. 25, 2025); see *PowerSchool*

*Information Security Report*, PowerSchool, [https://go.powerschool.com/rs/861-RMI-846/images/Cybersecurity\\_Report.pdf?version=2&utm\\_medium=social//?wtime](https://go.powerschool.com/rs/861-RMI-846/images/Cybersecurity_Report.pdf?version=2&utm_medium=social//?wtime) (last visited Aug. 25, 2025).

64. Further, PowerSchool was aware, or should have been aware, of the risks its deficient practices imposed against Texas schools, their teachers, and Texas school-aged children because of the recent trends in cyber-attacks. Large corporations responsible for collecting, maintaining, and securing PII, SPI, and other forms of sensitive data have been recent targets for threat actors. Well known breaches like those against T-Mobile, AT&T, Equifax, Uber, and more put companies like PowerSchool on notice. Further, school districts and education technology companies in-particular have become rising targets for cyber-attacks. *School ransomware attacks are on the rise. What can districts do?*, K-12Dive, <https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333/> (last visited Aug. 22, 2025).

#### **IV. PowerSchool’s Conduct Warrants the Maximum Imposition of Civil Penalties for Each Violation of ITEPA**

65. The State of Texas is entitled to recover civil penalties between \$2,000 and \$50,000 for each violation of the ITEPA. *See* Texas Bus. & Com Code § 521.151(a).

66. The facts described in ¶¶ 19-47, and 52-55 shall be considered by the jury when determining the civil penalties to impose for each violation of the DTPA. *See* Tex. Bus. & Com. Code § 17.47(g)(1)-(6).

##### **A. The Unprecedented Size, Scope, and Nature of PowerSchool’s December 2024 Breach**

67. On January 29, 2025, PowerSchool filed a Data Breach report with the Office of the Attorney General of Texas. The January filing disclosed the December 2024 Data breach and reported **790,362 Texas victims**. Ex. E Data Breach ID BR-0004072, *PowerSchool*. Then, on May

22, 2025, PowerSchool supplemented its Data Breach report, increasing their report to **881,249 Texas victims**. Ex. D. PowerSchool’s amended report was filed shortly after school districts were targeted with ransom offers regarding their students’ and teachers’ sensitive personal information. During that time, further media coverage indicated that the number of Texas victims of the December Breach was potentially much higher than PowerSchool has reported, stating that PII belonging to **836,940** school-aged children and teachers from Dallas Independent School District *alone* was exfiltrated. *See* Lawrence Abrams, *PowerSchool hacker claims they stole data of 62 million students*, BLEEPING COMPUTER (Jan. 22, 2025), <https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/>.

68. PowerSchool’s Data Breach Reports to the Office of the Attorney General of Texas include the categories of personal and sensitive information disclosed in the December Data Breach. The categories include, “Name of individual, Address; Social Security Number Information; Medical Information; [and] Date of Birth.” *See* Ex. E, D. On information and belief, the disclosed data included other highly sensitive information such as children’s bus-stop information, grades, and grade-point averages. *See e.g.* Christopher Brown, *PowerSchool Faces Suit Over Breach of Student, Teacher Data (1)*, BLOOMBERG LAW (January, 10, 2025), <https://news.bloomberglaw.com/privacy-and-data-security/powerschool-sued-over-december-breach-of-student-teacher-data>.

*B. PowerSchool's Dangerous Response to its December 2024 Breach*

69. In response to its December 2024 breach, PowerSchool falsely, misleadingly, and deceptively represented to Texas schools, their teachers, Texas school-aged children and their parents that their exfiltrated PII, SPI, and PHI was deleted when it was not.

70. On January 9, 2025, PowerSchool's Chief Information Security Officer ("CISO") Mishka McCowan hosted a webinar in which PowerSchool represented that it had negotiated and paid a ransom to cybercriminals to delete the exfiltrated data. Collier, *supra*.

71. Law enforcement agencies and cybersecurity experts discourage ransom payments. Ransom payments do not guarantee the deletion of breached data, in light of false video evidence and the modern ease of copying data. Ransom payments also encourage cyber criminals to continue their illicit practices. *See Ransomware Prevention and Response for CISOs*, FBI, (<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 22, 2025)).

72. Aware of these issues and citing to a video provided by the hackers, PowerSchool misrepresented to Texas consumers that the exfiltrated data was deleted during the January 9, 2025, webinar. Collier, *supra*.

73. Relying on PowerSchool's misrepresentations, Dallas Independent School District communicated to students, teachers, and parents that **"Again, PowerSchool shared that all downloaded data has been destroyed."** *PowerSchool Cybersecurity Incident*, Dallas Independent School District, <https://thehub.dallasisd.org/2025/01/13/powerschool-cybersecurity-incident/> (last visited Aug. 22, 2025).

*C. Texas school-aged children's and teachers' PII, SPI, and PHI were not deleted.*

74. In May 2025, schools in North Carolina, Canada, Oregon, and other states were targets of ransom demands from cyber criminals to prevent the publishing of PII, SPI, and PHI. The criminals provided a data sample that matched the data stolen and purportedly deleted in PowerSchool's December 2024 breach. *See* James Coker, *PowerSchool Admits Ransom Payment Amid Fresh Extortion Demands*, InfoSecurity-Magazine (May 9, 2025), <https://www.infosecurity-magazine.com/news/powerschool-ransom-payment/>. PowerSchool confirmed the futility of their initial ransom on May 7, writing to schools that "We sincerely regret these developments- it pains us that our customers are being threatened and re-victimized by bad actors." *Id.*

#### **VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT**

75. The State incorporates the foregoing allegations as if set forth fully herein.

76. Tex. Bus. & Com. Code § 17.47 authorizes the Consumer Protection Division to bring an action for temporary and permanent injunction whenever it has reason to believe that any person is engaged in, has engaged in, or is about to engage in any act or practice declared unlawful under Chapter 17 of the Business and Commerce Code.

#### **Count I**

##### **Engaging in false, misleading, or deceptive acts or practices in the conduct of any trade or commerce.**

77. Tex. Bus. & Com. Code § 17.46(a) prohibits "false, misleading, or deceptive acts or practices in the conduct of any trade or commerce."

78. As described above, PowerSchool has engaged in false, misleading, or deceptive acts or practices in violation of the DTPA.

## **Count II**

**Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not.**

79. Tex. Bus. & Com. Code § 17.46(b)(5) provides that “false, misleading, or deceptive acts or practices” includes “representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not.”

80. As described above, PowerSchool has engaged in false, misleading, or deceptive acts or practices by representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law in violation of the DTPA.

## **Count III**

**Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another**

81. Texas Bus. & Com. Code § 17.46(b)(7) provides that “false, misleading, or deceptive acts or practices” includes “representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another.”

82. As described above, PowerSchool has engaged in false, misleading, or deceptive acts or practices by representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another in violation of the DTPA.

#### **Count IV**

**Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.**

83. Tex. Bus. & Com. Code § 17.46(b)(24) provides that “false, misleading, or deceptive acts or practices” includes “failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.”

84. As described above, PowerSchool has engaged in false, misleading, or deceptive acts or practices by failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed in violation of the DTPA.

#### **VIOLATIONS OF THE IDENTITY THEFT ENFORCEMENT PROTECTION ACT**

85. Texas incorporates the foregoing allegations as if set forth fully herein.

86. Tex. Bus. & Com. Code § 521.151 authorizes the Attorney General to bring an action in the name of the state against a person to restrain a violation of ITEPA by a temporary restraining order or by a permanent or temporary injunction, or to recover civil penalties for each violation.

## **Count V**

### **Failing to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained in the regular course of business.**

87. Tex. Bus. & Com. Code § 521.052(a) requires businesses to “implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.”

88. As described above, PowerSchool has failed to implement and maintain reasonable security measures to protect from unlawful use or disclosure the sensitive personal information it collected or maintained in the regular course of business belonging to Texas schools, their teachers, and Texas school-aged children, in violation of the ITEPA.

## **CIVIL PENALTIES**

86. Texas incorporates the foregoing allegations as if set forth fully herein.

### **I. DTPA Civil Penalties**

86. The State of Texas is entitled to recover up to \$10,000 for each violation of the DTPA. Tex. Bus. & Com. Code § 17.47(c)(1).

87. Texas Bus. & Com. Code § 17.47(g) describes the six factors the trier of fact “shall consider” when determining the amount of civil penalties to impose: “(1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of any prohibited act or practice; (2) the history of previous violations; (3) the amount necessary to deter future violations; (4) the economic effect on the person against whom the penalty is to be assessed; (5) knowledge of the illegality of the act or practice; and (6) any other matter that justice may require.”

88. PowerSchool’s current financial situation must also be considered by the jury when determining civil penalties to impose. *See* Tex. Bus. & Com. Code § 17.47(g)(3)-(4), (6).

89. Texas is not required to allege injuries to bring claims seeking civil penalties under the DTPA. Tex. Bus. & Com. Code § 17.47(a) (creating a cause of action “[w]henever the consumer protection division has reason to believe that any person is engaging in, has engaged in, or is about to engage in any act or practice declared to be unlawful by [the DTPA] ...”); *see e.g.* *Holzman v. State*, No. 13-11-00168-CV, 2013 WL 398935, at \*3 (Tex. App.—Corpus Christi 2013, pet. denied) (“Moreover, it is not necessary for the State to allege any injury to a [consumer] to recover the civil penalties it seeks in its live petition.”); *see also Texas v. Colony Ridge, Inc.*, Civil Case No. CV-H-24-0941, 2024 WL 4553111, at \*8 (S.D. Tex. 2024) (same).

## **II. ITEPA Civil Penalties**

90. Tex. Bus. & Com. Code § 521.151(a) authorizes the attorney general to recover civil penalties “of at least \$2,000 but not more than \$50,000 for each violation.”

91. PowerSchool failed to implement and maintain reasonable procedures, and failed to take appropriate corrective action to protect sensitive personal information collected or maintained by PowerSchool in the regular course of business resulting in the theft of 881,249 Texans’ PII, SPI, and PHI in December of 2024. PowerSchool violated ITEPA for each and every Texan’s PII, SPI, and PHI exfiltrated.

92. In the alternative, as described above, PowerSchool provided education technology software services to 1,750 Texas schools. PowerSchool has represented to Texas that 71% percent of Texas schools had data exfiltrated. Therefore, 1,242 Texas schools had Texans’ PII, SPI, and PHI exfiltrated and PowerSchool violated ITEPA for each and every school that had data exfiltrated.

## **TRIAL BY JURY**

93. Texas demands a jury trial.

## **PRAYER FOR RELIEF**

NOW THEREFORE, the State respectfully prays that the Court enter a final judgment in its favor and issue an order the following:

- a. Finding that Defendants have violated §§ 17.46(a) and (b) of the DTPA by engaging in the false, misleading, or deceptive acts or practices alleged above;
  - b. Finding that Defendants have violated § 521.052(a) of the Texas Identity Theft Enforcement and Protection Act by engaging in the unlawful acts and practices alleged above;
  - c. Requiring Defendants to pay civil penalties of up to \$10,000 per violation of the DTPA as authorized by Tex. Bus. & Com. Code § 17.47(c)(1);
  - d. Requiring Defendants to pay at an additional penalty of between \$2,000 and \$50,000 for each violation of ITEPA as authorized by Tex. Bus. & Com. Code § 521.151(a);
  - e. Permanently enjoining Defendants from engaging in the above acts, practices, and conduct in trade or any other practice in violation of the DTPA or ITEPA, such injunctive relief being authorized by § 17.47 of the DTPA and § 521.151(b) of the ITEPA;
  - f. Requiring Defendants to pay all attorneys' fees and costs for the prosecution and investigation of this action, as authorized by Tex. Gov't Code Ann. § 402.006(c);
- and

- g. Ordering that the State be awarded any further relief to which it demonstrates entitlement under the law.

Respectfully submitted,

KEN PAXTON  
Attorney General of Texas

BRENT WEBSTER  
First Assistant Attorney General

RALPH MOLINA  
Deputy First Assistant Attorney General

AUSTIN KINGHORN  
Deputy Attorney General for Civil Litigation

JOHNATHAN STONE  
Chief, Consumer Protection Division

/s/John C. Hernandez

JOHN C. HERNANDEZ  
Assistant Attorney General  
State Bar No. 24095819

MATTHEW CHILDREY  
Assistant Attorney General  
State Bar No. 24138100

ADAM HOLTZ  
Assistant Attorney General  
State Bar No. 24143021  
Office of the Attorney General of Texas  
Consumer Protection Division  
300 W. 15th St.

Austin, Texas 78701  
Phone: (512) 463-2185  
Fax: (512) 473-8301

JC.Hernandez@oag.texas.gov  
Matt.Childrey@oag.texas.gov  
Adam.Holtz@oag.texas.gov

**ATTORNEYS FOR THE STATE**

# Exhibit A

**Students (ver3.6.1)**

This table maintains Student demographics and other School related information such as Lunch ID, Grade Level and scheduling data.

Column Name	Data Type	Description
Alert_Discipline (ver3.6.1)	Text	One of many various alerts in PowersSchool. This field stores the text tied to the alert.
Alert_DisciplineExpires (ver3.6.1)	Date	One of many various alerts in PowersSchool. This field stores the expiration date tied to the alert.
Alert_Guardian (ver3.6.1)	Text	One of many various alerts in PowersSchool. This field stores the text tied to the alert.
Alert_GuardianExpires (ver3.6.1)	Date	One of many various alerts in PowersSchool. This field stores the expiration date tied to the alert.
Alert_Medical (ver3.6.1)	Text	One of many various alerts in PowersSchool. This field stores the text tied to the alert.
Alert_MedicalExpires (ver3.6.1)	Date	One of many various alerts in PowersSchool. This field stores the expiration date tied to the alert.
Alert_Other (ver3.6.1)	Text	One of many various alerts in PowersSchool. This field stores the text tied to the alert.
Alert_OtherExpires (ver3.6.1)	Date	One of many various alerts in PowersSchool. This field stores the expiration date tied to the alert.
AllowWebAccess (ver3.6.1)	Integer	Whether to allow the parent user ID to log in to the parent/student page: 1=Yes 0=No
Applic_Response_Recvd_Date (ver3.6.1)	Date	No longer used. Application for free lunch response date.
Applic_Submitted_Date (ver3.6.1)	Date	No longer used. Application for free lunch date submitted.
Balance1 (ver3.6.1)	Real	Lunch balance.

Column Name	Data Type	Description
Balance2 (ver3.6.1)	Real	Beginning lunch balance for the year copied from balance 1 in the end-of-year process.
Balance3 (ver3.6.1)	Real	Fees balance.
Balance4 (ver3.6.1)	Real	Beginning fee balance for the year copied from balance 3 in the end-of-year process.
Building (ver4.0.0)	String 10	This field is necessary to capture the building value assigned in PowerScheduler to a student. This will need to be moved from Students:Sched_NextYearBuilding during the End-of-Year process. The field stores the text value of building (i.e. Building 1)
Bus_Route (ver3.6.1)	String 20	The district name for the students' bus route.
Bus_Stop (ver3.6.1)	String 20	The stop number at which the student gets on and off the bus.
CampusID (ver3.6.1)	Integer	No longer used by application. This field may still be referenced on reports and/or custom pages.
City (ver3.6.1)	String 50	City element of the students address.
ClassOf (ver3.6.1)	Integer	Stores the calculated graduation class year.
Cumulative_GPA (ver3.6.1)	Real	The cumulative GPA for the student as of the last time GPA calculations ran.
Cumulative_Pct (ver3.6.1)	Real	The cumulative percent GPA for the student as of the last time GPA calculations ran.
Custom (ver3.6.1)	Text	This field holds all the students' custom fields and their values in key-pair format separated by semicolons.
CustomRank_GPA (ver3.6.1)	Real	The rank for the student as of the last time GPA calculations ran based on their custom calculations.
DCID (ver4.0.0)	Integer	Unique identifier for this table. Indexed.

Column Name	Data Type	Description
DOB (ver3.6.1)	Date	Date of birth.
DistrictEntryDate (ver3.6.1)	Date	A static field with no coding used simply to hold information entered by the district.
<i>DistrictEntryGradeLevel</i> (ver3.6.1)	Integer	No longer used by application. This field may still be referenced on reports and/or custom pages.
DistrictOfResidence (ver3.6.1)	String 20	The school district in which the student physically lives.
Doctor_Name (ver3.6.1)	String 60	Name of the Doctor for the student.
Doctor_Phone (ver3.6.1)	String 30	Phone number for the Doctor.
Emerg_Contact_1 (ver3.6.1)	String 60	Name to contact in case of an emergency.
Emerg_Contact_2 (ver3.6.1)	String 60	Name to contact in case of an emergency.
Emerg_Phone_1 (ver3.6.1)	String 30	Phone number for the first emergency contact.
Emerg_Phone_2 (ver3.6.1)	String 30	Phone number for the second emergency contact.
Enroll_Status (ver3.6.1)	Integer	The enrollment status of the student. 0=Currently enrolled 1=Inactive 2=Transferred out 3=Graduated. Indexed.
EnrollmentCode (ver3.6.1)	Integer	This can be used for any special code that needs to be attached to an enrollment. Currently, it is only used in AZ: 0=None 1=CECA 2=CECB 3=Open Enrollment
EnrollmentType (ver3.6.1)	String 2	This is used to specify what type of enrollment the student has at this school. Currently, it is only used in AZ: M=Main A=Ancillary
Enrollment_SchoolID (ver3.6.1)	Integer	This field holds the school ID value when creating reenrollment records.
Enrollment_Transfer_Date_Pend (ver3.6.1)	Date	Date of the Pending transfer of the student from the school. If 00/00/00 then immediate transfer.
Enrollment_Transfer_Info (ver3.6.1)	Blob	Blob containing one or more comments regarding this transfer.

Column Name	Data Type	Description
EntryCode (ver3.6.1)	String 10	The code representing how or why the student entered school. These codes are stored in Gen Table [6] cat=entrycodes. These are set in school setup.
EntryDate (ver3.6.1)	Date	The date the student enrolled in school for the current enrollment. Indexed.
Ethnicity (ver3.6.1)	String 20	Heritage background of a student. The codes assigned here are stored in the Gen Table [6] Cat=Ethnicity. These are set in school setup.
Exclude_FR_Rank (ver3.6.1)	Boolean	True/False. Exclude from class rank. Used to keep particular students from counting in the class rank. This is often used for special education students.
ExitCode (ver3.6.1)	String 10	The code representing how or why the student exited the school. These codes are stored in Gen Table [6] cat=exitcodes. These are set in school setup.
ExitComment (ver3.6.1)	Text	Any comments for the student exiting this school.
ExitDate (ver3.6.1)	Date	The date the student exited for the current/last enrollment. This is the day after a student-attended class. For example, if the last day the student is in school is a Wednesday, Thursday is the exit day. Indexed.
FTEID (ver4.0.0)	Integer	The internal number for the FTE with which this record is associated. Indexed.
Family_Ident (ver3.6.1)	String 30	No longer used by application. This field may still be referenced on reports and/or custom pages.
Father (ver3.6.1)	String 60	Name of students father.
Father_StudentCont_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliancy. Indexed.
Fee_Exemption_Status (ver3.7.0)	Integer	Determines what fees this student is exempt from. Values are, 0 = Students Not Exempted1 = Students Exempted from Course Fees. 2 = Students Exempted from School Fees 3 = Students Exempted from All Fees.

Column Name	Data Type	Description
First_Name (ver3.6.1)	String 15	Students' first name.
FullTimeEquiv_obsolete (ver4.0.0)	Real	Changed name from FullTimeEquiv 4.0. This column is no longer used and instead FTEID is used. Originally, Full-time equivalency to determine if this is a full-time or part-time student. The largest number for this will usually be 1 and fractions are expressed as decimals such as .5 or .25.
Gender (ver3.6.1)	String 2	M=Male F=Female. Indexed.
GradReqSet (ver3.6.1)	String 3	No longer used by application. This field may still be referenced on reports and/or custom pages.
GradReqSetID (ver3.6.1)	Integer	The graduation requirements this student follows. Links to the ID on the GradReq Table [37].
Grade_Level (ver3.6.1)	Integer	The grade the student is in. Since this is an integer: 0=Kindergarten 1, -2=Preschool. Indexed.
Graduated_Rank (ver3.6.1)	Integer	Class rank upon the time of graduation.
Graduated_SchoolID (ver3.6.1)	Integer	Stores the school number the student graduated from so the user can search for him or her in the Graduated Students school.
Graduated_SchoolName (ver3.6.1)	String 60	Stores the name of the school the student graduated from so the user can search for him or her in the Graduated Students school.
GuardianEmail (ver3.6.1)	Text	Parent/guardian email address.
GuardianFax (ver3.6.1)	String 30	Parent/guardian fax number.
Guardian_StudentCont_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliancy. Indexed.
Home_Phone (ver3.6.1)	String 30	Home phone number for the student. Indexed.
Home_Room (ver3.6.1)	String 60	No longer used by application. This field may still be referenced on reports and/or custom pages.

Column Name	Data Type	Description
House (ver4.0.0)	String 10	This field is necessary to capture the house value assigned in PowerScheduler to a student. This will need to be moved from Students:Sched_NextYearHouse during the End-of-Year process. The field stores the text value of house (i.e. Hawthorne).
ID (ver3.6.1)	Integer	Sequential number generated by the application, but uniqueness in the table is not guaranteed. Indexed.
LDAPEnabled (ver4.3.0/5.0.7)	Integer	Used for LDAP support.
LastFirst (ver3.6.1)	String 35	Last, First, Mi. Indexed.
LastMeal (ver3.6.1)	String 20	Stores the date of last lunch purchase.
Last_Name (ver3.6.1)	String 20	Students last name.
Locker_Combination (ver3.6.1)	String 20	No longer used by application. This field may still be referenced on reports and/or custom pages.
Locker_Number (ver3.6.1)	String 15	No longer used by application. This field may still be referenced on reports and/or custom pages.
Log (ver3.6.1)	Text	Place to write notes about transferring students.
LunchStatus (ver3.6.1)	String 3	Represents the portion of lunch a student must pay for: Blank=No status P=Full pay R=Reducednt F=Free E=Exempt T=Temporary FDC=Free-DC.
Lunch_ID (ver3.6.1)	Real	The students PowerLunch number. Indexed.
Mailing_City (ver3.6.1)	String 50	City part of the mailing address.
Mailing_State (ver3.6.1)	String 2	State part of the mailing address.
Mailing_Street (ver3.6.1)	String 60	Street address of the mailing address.
Mailing_Zip (ver3.6.1)	String 10	The zip code in the students mailing address.
MembershipShare (ver3.6.1)	Real	The amount of a student's membership this school claims. If a student attends more than one school each one will only be able to claim a

Column Name	Data Type	Description
		certain portion of the membership. The largest number for this will usually be 1 and fractions expressed as decimals. Like .5 or .25.
Middle_Name (ver3.6.1)	String 20	Student's middle name.
Mother (ver3.6.1)	String 60	Name of students mother.
Mother_StudentCont_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliancy. Indexed.
Next_School (ver3.6.1)	Integer	The school the student will be attending the next school year. It is likely this will be the same school. The information is stored as the internal ID on the schools table for that school.
PL_Language (ver3.6.1)	String 12	Powerlink language, which is either Spanish or English.
Person_ID (ver 5.0.0)	Integer	The related person in the Relationship table. Indexed.
Phone_ID (ver3.6.1)	Integer	The number for the student on PowerLink. Indexed.
PhotoFlag (ver3.6.1)	Integer	Set to 1 if a photo exists for this student.
SDataRN (ver3.6.1)	Integer	No longer used by application. This field may still be referenced on reports and/or custom pages.
SSN (ver3.6.1)	String 12	Students Social Security number. Indexed.
Sched_LoadLock (ver5.0.0)	Boolean	This field will lock individual students' schedules from Load.
Sched_LockStudentsSchedule (ver3.6.1)	Boolean	True/False: True (selected)=Do not allow the schedule to be changed by PowerScheduler. False (deselected)=Schedule this student when the scheduling engine is run.
Sched_NextYearBuilding (ver3.6.1)	String 10	The building this student will be in next year for schools with multi-building needs.
Sched_NextYearBus (ver3.6.1)	String 20	No longer used by application. This field may still be referenced on reports and/or custom pages.

Column Name	Data Type	Description
Sched_NextYearGrade (ver3.6.1)	Integer	The grade the student is going to be in next year. If the student is being retained, this should be the same as the current grade level.
Sched_NextYearHomeRoom (ver3.6.1)	String 10	No longer used by application. This field may still be referenced on reports and/or custom pages.
Sched_NextYearHouse (ver3.6.1)	String 10	The house this student will belong to next year. This is used for scheduling purposes. A house is most often used for _school within a school_ type of scheduling.
Sched_NextYearTeam (ver3.6.1)	String 10	The team this student will belong to next year.
Sched_Priority (ver3.6.1)	Integer	Indicates when you want this student to be scheduled in relation to the other students. The lower the number, the sooner he or she is scheduled.
Sched_Scheduled (ver3.6.1)	Boolean	A flag indicating if this student has had a schedule built for them. True means they do have a schedule and another will not be made unless the engine is told to reschedule regardless of this flag. False, the engine will build a schedule for this student next time.
Sched_YearOfGraduation (ver3.6.1)	Integer	Year of graduation. This changes if the student fails or skips a grade.
SchoolEntryDate (ver3.6.1)	Date	A static field with no coding used to hold information entered by the district.
SchoolEntryGradeLevel (ver3.6.1)	Integer	Grade level of the student for entering into this school.
SchoolID (ver3.6.1)	Integer	This ID is linked to the School_Number from the School table. Indexed.
Simple_GPA (ver3.6.1)	Real	The simple GPA for the student as of the last time GPA calculations ran.
Simple_PCT (ver3.6.1)	Real	The simple percent GPA for the student as of the last time GPA calculations ran.
State (ver3.6.1)	String 2	State element of address.
State_EnrollFlag (ver3.6.1)	Boolean	True/False. Used for state reporting to indicate he or she is enrolled at the state level.

Column Name	Data Type	Description
State_ExcludeFromReporting (ver3.6.1)	Boolean	True/False. Used for state reports to exclude certain students from reports. Most often, these will be special education students who are reported differently.
State_StudentNumber (ver3.6.1)	String 32	The state-assigned student number for the student. In most cases, this number should stay the same from school to school.
Street (ver3.6.1)	String 60	Student's street address.
StudentPers_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliance. Indexed.
StudentPict_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliance. Indexed.
StudentsSchEnr_guid (ver4.0.0)	String 32	Globally Unique Identifier for this table for SIF compliance. Indexed.
Student_AllowWebAccess (ver3.6.1)	Integer	Allow student user webID to log in to parent/student page: 1=Yes 0=No
Student_Number (ver3.6.1)	Real	Student Number assigned by the school. Indexed.
Student_Web_ID (ver3.6.1)	String 20	The student user ID for logging in to Powerschool Parent. Indexed.
Student_Web_Password (ver3.6.1)	String 20	The password for Student_Web_ID.
SummersSchoioIID (ver5.0.7)	Integer	School Identifier for this Student's Summer School, if applicable.
SummersSchoolNote (ver5.0.7)	String 80	Notes specific to this Student's Summer School.
TeacherGroupID (ver3.6.1)	Integer	No longer used by application. This field may still be referenced on reports and/or custom pages.
Team (ver4.0.0)	String 10	This field is necessary to capture the team value assigned in Powerscheduler to a student. This will need to be moved from Students:Sched_NextYearTeam during the End-of-Year process. Sched_NextYearTeam captures the record ID from the Gen table (Cat = TeacherGroups). Current_Team cannot capture the ID since this record is part of Powerscheduler and may be changed when scheduling for a future year. An acceptable compromise is to capture the value instead (i.e. Blue) and store this.

Column Name	Data Type	Description
Track (ver3.6.1)	String 20	A-H or blank. This represents the times of year a student goes to school. This is most common with year-round schools.
TransferComment (ver3.6.1)	Text	A text field for the school administrator to write a note about the reason a student is being transferred.
TuitionPayer (ver3.6.1)	Integer	This is an integer code used to represent the tuition status of a student. For AZ: 1=State-funded 2=Privately paid or no tuition
WM_Address (ver3.6.1)	String 70	No longer used by application. This field may still be referenced on reports and/or custom pages. Indexed.
WM_CreateDate (ver3.6.1)	Date	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_CreateTime (ver3.6.1)	Time	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_Password (ver3.6.1)	String 20	No longer used. Only used in version fix method.
WM_Status (ver3.6.1)	String 10	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_StatusDate (ver3.6.1)	Date	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_TA_Date (ver3.6.1)	Date	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_TA_Flag (ver3.6.1)	String 3	No longer used by application. This field may still be referenced on reports and/or custom pages.
WM_Tier (ver3.6.1)	Integer	Web Mail. No longer used.
Web_ID (ver3.6.1)	String 20	The parent user ID for logging in to PowerSchool Parent. Indexed.
Web_Password (ver3.6.1)	String 20	The parent password for logging in to PowerSchool Parent.

Column Name	Data Type	Description
Withdrawal_Reason_Code (ver4.0.0)	String 3	Reason code provided when a student withdraws from school.
Zip (ver3.6.1)	String 10	Students zip code.

**StudentSchedulingResults (ver5.0.0)**

This table will be used to compute grade level percent schedules, school level percent schedules and to serach the students based on the percent schedules. In addition, this table can be used to compare the scheduling results between different builds.

Column Name	Data Type	Description
BuildID (ver5.0.0)	Integer	Build identifier associated with these results.
CoreSlots (ver5.0.0)	Integer	Number of core slots scheduled for this student.
DCID (ver5.0.0)	Integer	Unique identifier for this table. Indexed.
EnrolledSlots (ver5.0.0)	Integer	Number of slots scheduled for this student.
ID (ver5.0.0)	Integer	Sequential number generated by the application, but uniqueness in the table is not guaranteed. Indexed.
PrimeReqSatisfied (ver5.0.0)	Integer	Number of primary requests satisfied.
TotalRequests (ver5.0.0)	Integer	Number of course requests of this student.
TotalReqSatisfied (ver5.0.0)	Integer	Number of requests satisfied including alternates.
StudentID (ver5.0.0)	Integer	The internal number for the student with which this record is associated. Indexed.

**StudentTest (ver3.6.1)**

Lists all the tests a student has taken.

Column Name	Data Type	Description
-------------	-----------	-------------

# Exhibit B

## Teachers (ver7.8.0)

This view, formerly the Teachers table, provides the fields from the Teachers table.

**Note:** In the *PowerSchoolDataDictionaryTables*, the Teachers table is no longer used and has been renamed Teachers\_ncf31. The SchoolStaff table and Users table have been created in its place.



Column Name	Initial Version	Data Type	Description
AccessValue	7.8.0	CLOB	<i>[From Users]</i> No longer used by application. This field may still be referenced on reports and/or custom pages.  <b>Note:</b> Also known as Access.
AdminLDAPEnabled	7.8.0	Number	[From Users] Used for LDAP support (Administrator specific).
AllowLoginEnd	7.8.0	Number	[From Users] Time-restricted login. This is the end time that teachers can log in.
AllowLoginStart	7.8.0	Number	[From Users] Time-restricted login. This is the start of the time that teachers can log in.
Balance1	7.8.0	Float	[From SchoolStaff] Lunch ba

Column Name	Initial Version	Data Type	Description
Balance2	7.8.0	Float	[From SchoolStaff] Beginning lunch balance for the year, copied from balance 1 in the end-of-year process.
Balance3	7.8.0	Float	[From SchoolStaff] Fees balance.
Balance4	7.8.0	Float	[From SchoolStaff] Beginning fee balance for the year, copied from balance 3 in the end-of-year process.
CanChangeSchool	7.8.0	CLOB	[From Users] Semicolon delimited list of Schools.School_Number values the Admin can switch to when logged into the Admin portal.
City	7.8.0	Varchar2(40)	[From Users] City element of the users address.
<i>Classpua</i>	<i>7.8.0</i>	<i>CLOB</i>	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Custom	7.8.0	CLOB	[From SchoolStaff] This field holds all the teacher custom fields and their values.
DCID	7.8.0	Number	[From SchoolStaff] Unique identifier for this table. Indexed. Required.

Column Name	Initial Version	Data Type	Description
DefaultStudScrn	7.8.0	CLOB	[From Users] The student page the user wants to appear by default.
Email_Addr	7.8.0	Varchar2(50)	[From Users] Stores the teachers email address and is used for email notifications to the teacher, such as student enrollment information.
<i>Ethnicity</i>	7.8.0	Varchar2(20)	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
FedEthnicity	7.8.0	Number	[From Users] Numerical answer to the question "Is the staff member Hispanic or Latino?" Valid values: -1 = Default value, user has not yet made a selection, 0 = No, 1 = Yes, 2 = User-defined answer specified on the Federal Ethnicity and Race Settings page.
FedRaceDecline	7.8.0	Number	[From Users] Valid values: 0 = Value assigned by default or one or more values specified in the TeacherRace table, 1 = Declined to specify race (no rows should appear in the TeacherRace table).
First_Name	7.8.0	Varchar2(20)	[From Users] First name.

Column Name	Initial Version	Data Type	Description
GradebookType	7.8.0	Number	[From Users] Indicates the type of

GroupValue	7.8.0	Number	[From Users] The security group (from Gen table) this user belongs to in PowerSchool. This determines which pages the user has access to.
Home_Phone	7.8.0	Varchar2(20)	[From Users] Changed name from Home_phone. Home phone number for the staff member.
HomePage	7.8.0	CLOB	[From Users] The page that appears when logging in to PowerSchool.
Homerom	7.8.0	Varchar2(20)	[From Users] This string does appear on some pages but does not impact any calculations.
HomeSchoolID	7.8.0	Number	[From Users] The teacher's home school. This ID is linked to the School_Number from the School table. Indexed. Required.
ID	7.8.0	Number	[From SchoolStaff] Sequential number generated by the application, but uniqueness in the table is not guaranteed. Indexed.

Column Name	Initial Version	Data Type	Description
IPAddrRestrict	7.8.0	CLOB	[From Users] The list of IP addresses the user is allowed to log in from. If blank, he or she can log in from any IP address.
Last_Name	7.8.0	Varchar2(20)	[From Users] Last name.
LastFirst	7.8.0	Varchar2(40)	[From Users] Last, First, Mi. Indexed.
LastMeal	7.8.0	Varchar2(20)	[From Users] Stores the date of last lunch purchase.
Log	7.8.0	CLOB	[From SchoolStaff] Log file is updated with importing.
LoginID	7.8.0	Varchar2(20)	[From Users] The PowerSchool login name. Indexed.
Lunch_ID	7.8.0	Float	[From Users] The PowerLunch number. Indexed.
Maximum_Load	7.8.0	Number	[From Users] Maximum student load permissible for this Teacher.
Middle_Name	7.8.0	Varchar2(20)	[From Users] Middle name.
NameAsImported	7.8.0	Varchar2(40)	[From Users] Used as a matching tool when importing teacher information.
NoOfCurClasses	7.8.0	Number	[From SchoolStaff] No longer used by application. This field may st

Column Name	Initial Version	Data Type	Description
			<i>be referenced on reports and/or custom pages.</i>
Notes	7.8.0	CLOB	[From SchoolStaff] Miscellaneous notes.
<i>NumLogins</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Password	7.8.0	Varchar2(4000)	[From Users] The PowerSchool login password.
<i>PeriodsAvail</i>	<i>7.8.0</i>	<i>Varchar2(40)</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Photo	7.8.0	Number	[From Users] Set to 1 if a photo exists for this user.
PowerGradePW	7.8.0	Varchar2(20)	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
PreferredName	7.8.0	Varchar2(45)	[From Users] Name the user prefers to use.
PSAccess	7.8.0	Number	[From Users] Indicates if the user can log in to PowerSchool Admin. Valid values: 0 = No, 1 = Yes.

Column Name	Initial Version	Data Type	Description
PTAccess	7.8.0	Number	[From Users] Indicates if the user can log in to PowerTeacher. Valid values: 0 = No, 1 = Yes.
<i>Sched_ActivityStatusCode</i>	7.8.0	Varchar2(8)	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Sched_BuildingCode	7.8.0	Varchar2(10)	[From SchoolStaff] The building the teacher is in.
Sched_Classroom	7.8.0	Varchar2(10)	[From SchoolStaff] The classroom this teacher is in most of the time.
Sched_Department	7.8.0	Varchar2(10)	[From SchoolStaff] The department to which the teacher belongs.
Sched_Gender	7.8.0	Varchar2(2)	[From SchoolStaff] Valid values: M = Male, F = Female.
Sched_Homeroom	7.8.0	Varchar2(10)	[From SchoolStaff] The teachers' homeroom.
Sched_HouseCode	7.8.0	Varchar2(10)	[From SchoolStaff] The house to which the teacher belongs.
Sched_IsTeacherFree	7.8.0	Number	[From SchoolStaff] Flag stating whether the teacher is always free. True=no limit on how many courses a teacher can teach at a time, most often used with fake or

Column Name	Initial Version	Data Type	Description
			SPED teachers. False= teacher can only teach one class at a time unless other wise specified at the course level.
Sched_Lunch	7.8.0	Number	[From SchoolStaff] Identifies the teacher to the engine as one who should be assigned a lunch period for each valid lunch day (according to the lunch courses valid days) when automated lunch is scheduled. This flag is used in lieu of creating course assignments for lunch.
Sched_MaximumConsecutive	7.8.0	Number	[From SchoolStaff] The most courses a teacher can teach in a row without a break.
Sched_MaximumCourses	7.8.0	Number	[From SchoolStaff] The maximum number of courses the teacher can teach.
<i>Sched_MaximumDuty</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Sched_MaximumFree	7.8.0	Number	[From SchoolStaff] The maximum number of preparatory periods the teacher can have.
Sched_MaxPers	7.8.0	Number	[From SchoolStaff] Reflects a long-standing setting in the


Column Name	Initial Version	Data Type	Description
			Engine for Max Periods Per Day the Teacher is to be scheduled.
Sched_MaxPreps	7.8.0	Number	[From SchoolStaff] Reflects the setting in the Engine for Max Prep Codes (per Term) a Teacher is to be scheduled.
<i>Sched_PrimarySchoolCode</i>	<i>7.8.0</i>	<i>Varchar2(10)</i>	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Sched_Scheduled	7.8.0	Number	[From SchoolStaff] Flag indicating whether or not this user is used for scheduling: True=Is used for scheduling. False=Not used for scheduling.
<i>Sched_Substitute</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>Sched_TeacherMoreOneSchool</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Sched_Team	7.8.0	Varchar2(12)	[From SchoolStaff] The team the teacher is on.
<i>Sched_TotalCourses</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From SchoolStaff] No longer used by application. This field may still</i>

Column Name	Initial Version	Data Type	Description
			<i>be referenced on reports and/or custom pages.</i>
<i>Sched_UseBuilding</i>	7.8.0	Number	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>Sched_UseHouse</i>	7.8.0	Number	<i>[From SchoolStaff] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
School_Phone	7.8.0	Varchar2(20)	[From Users] Changed name from School_phone. Phone number at the school assigned to this staff member. Not currently used by any application code.
SchoolID	7.8.0	Number	[From SchoolStaff] This ID is linked to the School_Number from the School table. Indexed.
SIF_StatePrID	7.8.0	Varchar2(32)	[From Users] Used by the PowerSchool SIF Agent that requires a state-level unique identifier for teachers. To be used in the SIF StaffPersonal object.
SSN	7.8.0	Varchar2(12)	[From Users] This users Social Security number.
StaffPers_GUID	7.8.0	Varchar2(32)	[From Users] Globally unique identifier for this table for SIF

Column Name	Initial Version	Data Type	Description
			compliance. Indexed.
StaffStatus	7.8.0	Number	[From SchoolStaff] Current title for staff. Valid values: 0 = Not Assigned, 1 = Teacher, 2 = Staff, 3 = Lunch Staff, 4 = Substitute. Indexed.
State	7.8.0	Varchar2(2)	[From Users] State element of the users address.
Status	7.8.0	Number	[From SchoolStaff] Indicates whether the teacher is active or not. Valid values: 1 = Current, 2 = No longer here. Indexed.
Street	7.8.0	Varchar2(80)	[From Users] Street element of the users address.
SupportContact	7.8.0	Number	[From Users] Value of 1 indicates that this user is an authorized support contact.
TeacherLDAPEnabled	7.8.0	Number	[From Users] Used for LDAP support (teacher specific).
TeacherLoginID	7.8.0	Varchar2(20)	[From Users] The login name for PowerTeacher.
TeacherLoginIP	7.8.0	CLOB	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>

Column Name	Initial Version	Data Type	Description
TeacherLoginPW	7.8.0	Varchar2(4000)	[From Users] The login password for PowerTeacher.
TeacherNumber	7.8.0	Varchar2(20)	[From Users] The number the district assigns to track the teacher.
Title	7.8.0	Varchar2(40)	[From Users] Stores a title name for the teacher and is used for sorting purposes.
Users_DCID	7.8.0	Number	[From Schoolstaff] Internal number for the associated User record. Indexed. Required.
WM_Address	7.8.0	Varchar2(70)	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
WM_Alias	7.8.0	Varchar2(70)	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
WM_CreateDate	7.8.0	Date	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
WM_CreateTime	7.8.0	Number	<i>[From Users] No longer used by application. This field may still be</i>

Column Name	Initial Version	Data Type	Description
			<i>referenced on reports and/or custom pages.</i>
<i>WM_Exclude</i>	<i>7.8.0</i>	<i>Number</i>	<i>[From Users] No longer used. Used in one Version fix method.</i>
<i>WM_Password</i>	<i>7.8.0</i>	<i>Varchar2(20)</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>WM_Status</i>	<i>7.8.0</i>	<i>Varchar2(10)</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>WM_StatusDate</i>	<i>7.8.0</i>	<i>Date</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>WM_TA_Date</i>	<i>7.8.0</i>	<i>Date</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
<i>WM_TA_Flag</i>	<i>7.8.0</i>	<i>Varchar2(3)</i>	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>

Column Name	Initial Version	Data Type	Description
 WM_Tier	7.8.0	Number	<i>[From Users] No longer used by application. This field may still be referenced on reports and/or custom pages.</i>
Zip	7.8.0	Varchar2(10)	[From Users] Zip code element of the users address.

# Exhibit C



## **STUDENT DATA PRIVACY AGREEMENT**

**STATE: TEXAS**

**PROCESSOR:**      **PowerSchool Group, LLC**

# **STANDARD STUDENT DATA PRIVACY AGREEMENT**

**TX-NDPA v1r6**

**School District or LEA**

Amarillo Independent School District

**and**

**Provider**

PowerSchool Group LLC

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

[Amarillo Independent School District], located at [7200 I-40 West Amarillo TX 79106 (the "**Local Education Agency**" or "**LEA**")

and

[PowerSchool Group LLC], located at 150 Parkshore Dr., Folsom, CA 95630 (the "**Provider**").

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

**2. Special Provisions. Check if Required**

- |   |  |
|---|--|
| X | If checked, the Supplemental State Terms and attached hereto as <b>Exhibit "G"</b> are hereby incorporated by reference into this DPA in their entirety. |
| X | If checked, LEA and Provider agree to the additional terms or modifications set forth in <b>Exhibit "H". (Optional)</b>                                  |
| X | If checked, the Provider, has signed <b>Exhibit "E"</b> to the Standard Clauses, otherwise known as General Offer of Privacy Terms                       |
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
  4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.
  5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
  6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Daniel West Title: CFO

Address: 7200 I-40 West Amarillo, TX 79106

Phone: 806-326-1000

Email: daniel.west@amaisd.org

The designated representative for the Provider for this DPA is:

Name: Darron Flagg

Title: Chief Compliance & Privacy Officer

Address: 150 Parkshore Drive, Folsom, CA 95630

Phone: 877-873-1550

Email: legalnotices@powerschool.com

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

LEA:

By: 

Date: 9/17/24

Printed Name: DANIEL WEST

Title/Position: CFO

Provider:

By: 

Date: September 16, 2024

Printed Name: Eric Shander

Title/Position: Chief Financial Officer

**STANDARD CLAUSES**

Version 1.0

**ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

**ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

**ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
  - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
  - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

- 1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
- 2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
- 3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between

**Exhibit "H"**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

The description of the PowerSchool products can be found at:

[https://www.powerschool.com/wp-content/uploads/PowerSchool-Service-Agreements/EXHIBIT\\_A\\_Product\\_Descriptions.pdf](https://www.powerschool.com/wp-content/uploads/PowerSchool-Service-Agreements/EXHIBIT_A_Product_Descriptions.pdf)

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

The data elements for the PowerSchool products can be found at:

[https://www.powerschool.com/wp-content/uploads/PowerSchool-Service-Agreements/EXHIBIT\\_B\\_Total.pdf](https://www.powerschool.com/wp-content/uploads/PowerSchool-Service-Agreements/EXHIBIT_B_Total.pdf)

**EXHIBIT “C”****DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Student Generated Content:** The term “Student-Generated Content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"****DIRECTIVE FOR DISPOSITION OF DATA**

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

**1. Extent of Disposition**

☐ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[ ]

☐ Disposition is Complete. Disposition extends to all categories of data.

**2. Nature of Disposition**

☐ Disposition shall be by destruction or deletion of data.

☐ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[ ]

**3. Schedule of Disposition**

Data shall be disposed of by the following date:

☐ As soon as commercially practicable.

☐ By [ ]

**4. Signature**

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

**5. Verification of Disposition of Data**

\_\_\_\_\_  
Authorized Representative of Provider


\_\_\_\_\_  
Date

**EXHIBIT "E"****GENERAL OFFER OF PRIVACY TERMS****1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [Amarillo Independent School District] ("Originating LEA") which is dated September 9, 2024, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: legalnotices@powerschool.com.

**[NAME OF PROVIDER]**

PowerSchool Group, LLC

Signature: 

Printed Name: Eric Shander

Date: September 16, 2024

Title/Position: Chief Financial Officer

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Amarillo Independent School District and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA:**

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

**DESIGNATED REPRESENTATIVE OF LEA:**

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_ Email: \_\_\_\_\_

**EXHIBIT "F"****DATA SECURITY REQUIREMENTS****Adequate Cybersecurity Frameworks****2/24/2020**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by PowerSchool Group LLC.

**Cybersecurity Frameworks**

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input checked="" type="checkbox"/>	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G"****Supplemental SDPC State Terms for Texas**

Version 1.0

This **Exhibit "G"**, as amended by Exhibit H, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [Amarillo Independent School District] (the "Local Education Agency" or "LEA") and [PowerSchool Group LLC] (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.
2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.
3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

~~**Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.~~

**Consider Provider as School Official.** The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider's obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

5. **Modification to Article VII, Section 4 of the DPA.** Article VI, Section 4 of the DPA (Annual Notification of Rights.) is amended as follows:

**Entire Agreement.** This DPA and the ~~Service Agreement~~ constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:
- Providing notification to the employees or parents of those students whose LEA Data was compromised and regulatory agencies or other entities as required by law or contract;
  - Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;
  - Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
  - Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.
7. **No Exhibit E without unaltered DPA including Texas Addendum.** Any alterations are only allowed in **Exhibit "H"**. Any terms under **Exhibit "H"** do not apply to **Exhibit "E"** and render **Exhibit "E"** null and void.

**EXHIBIT "H"****Additional Terms or Modifications**

Version 1.0

LEA and Provider agree to the following additional terms and modifications:

Notwithstanding anything in the contrary in the DPA or other Exhibits thereto, LEA and Provider agree to the following terms and modifications:

1. With respect to the DPA's **STANDARD CLAUSES**:

- 1.1. **Article II, ¶ 1. (Student Data Property of LEA)** is amended by striking ", including any modifications or additions or any portion thereof from any source,"
- 1.2. **Article IV, ¶ 4. (No Disclosure)** is amended by striking the word "of" and replacing with the word "or" in the sentence "This prohibition against disclosure shall not apply to aggregate summaries of Deidentified information."
- 1.3. **Article IV, ¶ 5. (De-Identified Data)** is amended by striking "and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer."

1.4. **Article V, ¶ 2 (Audits)** is amended as follows:

1.4.1 By removing the first sentence in the paragraph: "No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA" and replacing it with: "Provider's security compliance is assessed by independent third-party auditors. Upon LEA agreeing to an NDA, Provider shall provide access to information regarding Provider's ISO 27001:2103 certification and SOC II Reports. To the extent that Provider discontinues a third-party audit, Provider will adopt or maintain an equivalent industry-recognized security standard."

1.4.2 In the second sentence should read as follows:

"The Provider will cooperate reasonably with local, state, or federal agency with oversight authority or jurisdiction in connection with any investigation of the Provider and/or delivery of Services to students and/or LEA."

1.4.3 The last sentence replaces the word "shall" with the word "may".

- 1.5. **Article V, ¶ 4 (Data Breach) Section (5)** the word "reasonably" is added in front of the word "cooperate".
- 1.6. **Article VII, ¶ 1 (Termination)** The second sentence should read "In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, or writing, the terms of this DPA shall apply and take precedence."
- 1.7. **Article VII, ¶ 3 (Priority of Agreements)** The second sentence is amended by striking ", license agreement,".

- 1.8. **Article VI, ¶ 7 (Successors Bound)** is amended by striking the entire paragraph and replacing it with the following language:

"This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Only where the data processor entity changes such notice will include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement."

- 1.9. **Article VI, ¶ 8 (Authority)** is amended by striking "all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof."

2. With respect to the DPA's **EXHIBIT "C" DEFINITIONS**:

2.1 **Metadata**: is amended by adding a "." between the first and second sentences.

2.2 **Student Data**: is amended by striking the sentence "Student Data includes Meta Data."

2.3 **Targeted Advertising**: is amended by adding "or a higher education institution's response to a student's search for higher education institutions using an LEA provided student account." at the end of the paragraph.

3. With respect to the DPA's **EXHIBIT "G" SUPPLEMENTAL SDPC STATE TERMS FOR TEXAS**:

3.1 First Paragraph, first sentence should read, "This **Exhibit "G"**, as amended by **Exhibit "H"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms")"

3.2 **¶ 3. (Modification to Article III, Section 2 of the DPA)** Article III, Section 2 of the DPA (Annual Notification of Rights) is amended by deleting the entire paragraph "**Annual Notification of Rights.**" And replacing it with the following:

**"Consider Provider as School Official.** The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA."

3.3 Section 5 "and the Service Agreement" is added back into first sentence.

3.4 Section 6. **Reimbursement of Expenses Associated with Security Breach.** The first portion of the sentence is to read as follows:

"In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for direct costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with: ....."

3.7 **¶ 7. (No Exhibit E without unaltered DPA including Texas Addendum)** The first and last sentence are deleted to read:

"Any alterations are only allowed in **Exhibit "H"**."

# Exhibit D



- [Close Window](#)
- [Print This Page](#)
- [Expand All](#) | [Collapse All](#)

## BR-0004310

Data Breach ID	BR-0004310	Owner	Melissa de Pau Drousche
Status	Published at AG website	Submitted by CPD	<input type="checkbox"/>
Published at AG website Date	5/22/2025	Published at AG 12 months	5/22/2026
Unpublish Date	5/22/2026	Will Unpublish In Less Than 30 Days	<input type="checkbox"/>

### ▼ PART A - IDENTIFYING INFORMATION OF ENTITY THAT EXPERIENCED THE BREACH

Report Type	Supplemental	Business or Organization Mailing Address	150 Parkshore Dr.
Business or Organization Name	PowerSchool Group LLC	Business or Organization City	Folsom
Type of Business or Organization	Business - Sales of Goods or Services	State	California
Other - Please describe		Business or Organization Zip Code	95630
		Business or Organization Website	

### ▼ PART B - DETAILED DESCRIPTION OF THE NATURE AND CIRCUMSTANCES OF THE BREACH

Date breach discovered	12/28/2024	Types of Breach	Systems breach – Credential compromise
Start date of breach	12/19/2024	Location of Breached Information	Cloud Storage
End date of breach	12/28/2024	Information Encrypted	No
Types of Personal Information Involved	Name of individual; Address; Social Security Number Information; Medical Information; Date of Birth	Encryption Keys Compromised	

### ▼ PART C - MEASURES TAKEN BY THE PERSON OR ENTITY REGARDING THE BREACH

Notice of Breach provided to consumers	Yes	Notice delayed because of a Law Enforc ?	
Method of Notice	Email; Posted at company website or special website	Number of Texas Notified by Mail	
Additional measures to be taken	Enhanced Data Security Measures; Offer of Credit Monitoring to affected individuals	Number of Texas Notified by Email	881,249
Planned Notification Date			

### ▼ PART D - NUMBER OF RESIDENTS OF THIS STATE AFFECTED BY THE BREACH

Number of Texans affected by the breach	881,249	Total Number of Individuals Affected	48,469,371
---	---------	--------------------------------------	------------

▼ **PART E - NOTIFIED ANOTHER LAW ENFORCEMENT AGENCY**

Law Enforcement Agency Notified	Yes	Name of Agency Representative	Doug Domin
Name of Agency	FBI	Email of Agency Representative	djdomin@fbi.gov
Phone Number of Agency representative			

▼ **PART F - Submitter Information**

Submitter Name	Edward McNicholas	Submitter Phone	2025084779
Submitter Address	2099 Pennsylvania Avenue NW	Submitter Email	edward.mcnicholas@ropesgray.com
Submitter City	Washington	Submitter Relationship	Attorney
Submitter State	District of Columbia	Submitter Zip Code	20006

▼ **Follow-up Information**

Follow-up Contact Name	Edward McNicholas	Follow-up Contact Address	2099 Pennsylvania Avenue NW
Follow-up Contact Phone Number	2025084779	Follow-up Contact City	Washington
Follow-up Contact Email	edward.mcnicholas@ropesgray.com	Follow-up Contact State	District of Columbia
Follow-up Relationship	Attorney	Follow-up Contact Zip code	20006

▼ **Signature**

Statement agreement	<input checked="" type="checkbox"/>	Signature Full Name	Edward McNicholas
---------------------	-------------------------------------	---------------------	-------------------

▼ **System Information**

Created By	Data Security Breach Reporting system Site Guest User, 5/20/2025, 10:29 PM	Last Modified By	Jared Anthony, 5/22/2025, 7:38 AM
------------	--	------------------	-----------------------------------

**Data Security Breach Report History**

5/22/2025, 7:38 AM

User	Jared Anthony
Action	Changed <b>Unpublish Date</b> to 5/22/2026. Changed <b>Published at AG website Date</b> to 5/22/2025. Changed <b>Status</b> from Pending Review to <b>Published at AG website</b> .

5/20/2025, 10:29 PM

User	Data Security Breach Reporting system Site Guest User
Action	Created.

# Exhibit E



- [Close Window](#)
- [Print This Page](#)
- [Expand All](#) | [Collapse All](#)

## BR-0004072

Data Breach ID	BR-0004072	Owner	Melissa de Pau Drousche
Status	Unpublished from AG Website	Submitted by CPD	<input type="checkbox"/>
Published at AG website Date	1/29/2025	Published at AG 12 months	1/29/2026
Unpublish Date	1/29/2026	Will Unpublish In Less Than 30 Days	<input type="checkbox"/>

### ▼ PART A - IDENTIFYING INFORMATION OF ENTITY THAT EXPERIENCED THE BREACH

Report Type	Initial	Business or Organization Mailing Address	150 Parkshore Dr.
Business or Organization Name	PowerSchool Group LLC	Business or Organization City	Folsom
Type of Business or Organization	Business - Sales of Goods or Services	State	California
Other - Please describe		Business or Organization Zip Code	95630
		Business or Organization Website	

### ▼ PART B - DETAILED DESCRIPTION OF THE NATURE AND CIRCUMSTANCES OF THE BREACH

Date breach discovered	12/28/2024	Types of Breach	Systems breach – Credential compromise
Start date of breach	12/19/2024	Location of Breached Information	Cloud Storage
End date of breach	12/28/2024	Information Encrypted	No
Types of Personal Information Involved	Name of individual; Address; Social Security Number Information; Medical Information; Date of Birth	Encryption Keys Compromised	

### ▼ PART C - MEASURES TAKEN BY THE PERSON OR ENTITY REGARDING THE BREACH

Notice of Breach provided to consumers	No	Notice delayed because of a Law Enforc ?	No
Method of Notice		Number of Texas Notified by Mail	
Additional measures to be taken	Enhanced Data Security Measures; Offer of Credit Monitoring to affected individuals	Number of Texas Notified by Email	
Planned Notification Date	1/29/2025		

### ▼ PART D - NUMBER OF RESIDENTS OF THIS STATE AFFECTED BY THE BREACH

Number of Texans affected by the breach	790,362	Total Number of Individuals Affected	0
---	---------	--------------------------------------	---

▼ **PART E - NOTIFIED ANOTHER LAW ENFORCEMENT AGENCY**

Law Enforcement Agency Notified	Yes	Name of Agency Representative	Doug Domin
Name of Agency	FBI	Email of Agency Representative	djdomin@fbi.gov
Phone Number of Agency representative			

▼ **PART F - Submitter Information**

Submitter Name	Edward McNicholas	Submitter Phone	2025084779
Submitter Address	2099 Pennsylvania Avenue NW	Submitter Email	edward.mcnicholas@ropesgray.com
Submitter City	Washington	Submitter Relationship	Attorney
Submitter State	District of Columbia	Submitter Zip Code	20006

▼ **Follow-up Information**

Follow-up Contact Name	Edward McNicholas	Follow-up Contact Address	2099 Pennsylvania Avenue NW
Follow-up Contact Phone Number	2025084779	Follow-up Contact City	Washington
Follow-up Contact Email	edward.mcnicholas@ropesgray.com	Follow-up Contact State	District of Columbia
Follow-up Relationship	Attorney	Follow-up Contact Zip code	20006

▼ **Signature**

Statement agreement	<input checked="" type="checkbox"/>	Signature Full Name	Edward McNicholas
---------------------	-------------------------------------	---------------------	-------------------

▼ **System Information**

Created By	Data Security Breach Reporting system Site Guest User, 1/27/2025, 9:11 PM	Last Modified By	Jared Anthony, 5/22/2025, 7:37 AM
------------	---	------------------	-----------------------------------

**Data Security Breach Report History****5/22/2025, 7:37 AM**

User	Jared Anthony
Action	<b>Changed Status</b> from Published at AG website to <b>Unpublished from AG Website</b> .

**1/29/2025, 9:14 AM**

User	Jared Anthony
Action	<b>Changed Unpublish Date</b> to <b>1/29/2026</b> . <b>Changed Published at AG website Date</b> to <b>1/29/2025</b> . <b>Changed Status</b> from Pending Review to <b>Published at AG website</b> .

**1/29/2025, 9:14 AM**

User	Jared Anthony
Action	<b>Deleted 1/29/2026 in Unpublish Date</b> . <b>Deleted 1/29/2025 in Published at AG website Date</b> . <b>Changed Unpublish Date</b> to <b>1/29/2026</b> . <b>Changed Published at AG website Date</b> to <b>1/29/2025</b> .

**1/27/2025, 9:11 PM**

User	Data Security Breach Reporting system Site Guest User
Action	<b>Created</b> .

Copyright © 2000-2025 salesforce.com, inc. All rights reserved.