DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

RIDER

This is a Rider to the contract (including any terms of services or terms of use or any other policies, terms, agreements, or understandings referenced therein) between the Commack Union Free School District ("the District") and TPW Inc/I Know It ("the Contractor"), that is being entered into for a Three year term for the use of I Know It.com pursuant to the attached quote ("the Contract")(collectively, the Contract and Rider are referred to as "the Agreement").

To the extent that the provisions of this Rider and the annexed Data Privacy Agreement are inconsistent with any terms set forth in the Contract, the provisions of this Rider and the annexed Data Privacy Agreement will control.

1. Plan for Security and Protection of Personally Identifiable Information

A. "District Data" means all information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to this Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except PII from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

B. "Personally Identifiable Information" or "PII" includes, but is not limited to: (i) a person's name or address or the names or addresses of a student's parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or Contractor reasonably believes knows the identity of the person to whom a record relates.

C. The Contractor represents and warrants that it will comply with all District policies and State, federal and local laws, regulations, rules and requirements related to the confidentiality, security and privacy of District Data.

D. The Contractor represents and warrants that District Data received by the Contractor will be used only to perform Contractor's obligations pursuant to the Agreement and for no other purpose.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

E. The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use services provided by the Contractor pursuant to the Agreement) that is necessary to fulfill the Contractor's duties pursuant to the Agreement.

F. The Parties agree that all rights including all intellectual property rights in and to District Data will remain the exclusive property of the District and that the Contractor has a limited, non-exclusive license to use District Data solely to perform the Services pursuant to the Agreement.

G. If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of the Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials.

H. The Contractor must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit A simultaneously with the execution and delivery of this Rider. The terms of the Data Privacy Agreement are hereby incorporated into this Rider.

I. All the provisions of this Paragraph will survive the expiration or sooner termination of the Agreement.

2. Indemnification by the District: If the Contract has any provision that requires the District to indemnify, defend and/or hold harmless the Contractor, such provision will be void and have no force or effect.

3. Entire Agreement/No End User Agreements: The Agreement contains the entire agreement of the parties with respect to the subject matter thereof and supersedes any and all other agreements, understandings and representations, written or oral, by and between the parties. In the event that any part of the Agreement references terms of service or terms of use or any other policies, terms, agreements or understandings, the applicable policies, terms, agreements or understandings are those that were in effect on the date of the Contract, unless the applicable policies, terms, agreements or understandings were modified pursuant to Paragraph 6 of this Rider. In the event that the Consultant requires District employees or other End Users to enter into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, those agreements and/or understandings will be null, void and without effect, and the terms of the Agreement will apply.

4. Termination: The Agreement may be terminated by the District immediately upon the Contractor's breach of the Contractor's obligations set forth in paragraph 1 of this Rider. Upon termination of the Agreement, the Contractor is not entitled to any further payments hereunder.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

5. Notices: Any notices required or permitted to be given pursuant to the terms of the Agreement must be in writing and either personally delivered or sent by nationally recognized overnight carrier to the parties at the following addresses:

To the Contractor:
TPW Inc/I Know It

To the District:
Commack Union Free School District
PO Box 150
Commack, NY 11725
Attention: Superintendent of Schools

With a copy to:
Lamb & Barnosky, LLP
534 Broadhollow Road, Suite 210
P.O. Box 9034
Melville, New York 11747
Attention: Eugene R. Barnosky, Esq.

If the notice is sent by personal mail, it will be deemed delivered upon receipt and if sent by registered or certified mail, it shall be deemed delivered 3 days after so mailing.

6. Modification: The Agreement may not be changed by any District Employee or other End User. The Agreement may not be changed orally, electronically, by click-through agreement, or by continued use. The Agreement may only be changed by an agreement in writing signed by the District. Any waiver of any term, condition or provision of the Agreement will not constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition or provision constitute a waiver of any subsequent or succeeding breach.

7. Governing Law, Choice of Forum and Waiver of Jury Trial: The Agreement is subject to, governed by, enforced according to and construed according to the laws of the State of New York, without regard to the conflicts of laws provisions thereof. Notwithstanding the arbitration provisions in the Contract, if any, the parties agree that any dispute arising under the Agreement will be litigated in a New York State Court in Suffolk County, New York. The parties each waive trial by jury in any action concerning the Agreement.

8. No Assignment: In accordance with the provisions of New York General Municipal Law § 109, the Contractor is hereby prohibited from assigning, transferring, conveying, subletting or otherwise disposing of the Agreement, or of the Contractor's rights, title, or interest in the Agreement, or the Contractor's power to execute the Agreement to any other person or corporation without the previous consent in writing from the District.

9. Third-Party Beneficiaries: There are no third-party beneficiaries in the Agreement.

10. Execution: This Rider may be executed in one or more counterparts, all of which

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

shall be considered one and the same agreement. This Rider may be executed by facsimile or PDF signature, each of which shall constitute an original for all purposes.

11. Notwithstanding the execution of this Rider or any other term or condition of this Rider, it will not become effective unless and until the Contract between the parties is in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement.

Commack Union Free School District

By: DocuSigned by: Alise Pulliam 736E7C729E52437...

Alise Pulliam
Executive Director for Instructional Technology

TPW Inc/I Know It , **the Contractor**

By: DocuSigned by: Jason Slater 10C2B3D5B8E54D0...

Name: Jason Slater
Title: IT Director

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

EXHIBIT A

DATA PRIVACY AGREEMENT

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

COMMACK UNION FREE SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and TPW Inc/I Know It ("the Contractor"), collectively, “the Parties.”

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms have the following meanings:

1. Breach: The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information of District Data, or a breach of the Contractor’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.

2. Commercial or Marketing Purpose: The sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.

3. Disclose: To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.

4. District Data: All information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to the Service Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except Personally Identifiable Information from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

5. Education Record: An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

6. Educational Agency: As defined in Education Law 2-d, a school district, board of cooperative educational services, School, or the New York State Education Department.

7. Eligible Student: A student who is eighteen years of age or older.

8. Encrypt or Encryption: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR § 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

9. NIST Cybersecurity Framework: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

10. Parent: A parent, legal guardian or person in parental relation to the Student.

11. Personally, Identifiable Information ("PII"): Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

12. Release: Has the same meaning as Disclose.

13. Service Agreement:

The agreement between the District and the Contractor with an effective date of July 1, 2022.

14. Services: The services provided by the Contractor to the District pursuant to the Service Agreement.

15. School: Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

16. Student: Any person attending or seeking to enroll in an Educational Agency.

17. Student Data: Personally, Identifiable Information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g. Personally Identifiable Information includes, but is not limited to: (i) a person's name or address or the names or addresses of a Student's parents or other family members; (ii) any personal identifier (*e.g.,* SSN, student number or biometric record); (iii) indirect identifiers (*e.g.,* date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the District community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or the Contractor reasonably believes know the identity of the person to whom a record relates.

18. Subcontractor: The Contractor's non-employee agents, consultants and/or other persons or entities not employed by the Contractor who are engaged in the provision of Services pursuant to the Service Agreement.

19. Teacher or Principal APPR Data: Personally, Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to Release pursuant to the provisions of Education Law §§ 3012-c and 3012-d.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for the Contractor to provide Services to the District pursuant to the Service Agreement; the Contractor may receive District Data regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C.§§ 6501-6506 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. § 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); New York Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law and to protect District Data. The Contractor agrees to maintain the confidentiality and security of District Data in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

The Contractor has no property or licensing rights or claims of ownership to District Data, and the Contractor must not use District Data for any purpose other than to provide the Services set forth in the Service Agreement. The Contractor agrees that neither the Services provided to the District nor the manner in which the Services are provided by the Contractor will violate applicable New York, federal and local laws, rules and regulations.

If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of this Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

3. Collection of Data.

The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use the Services) that is necessary to fulfill the Contractor's duties pursuant to the Service Agreement.

4. Data Security and Privacy Plan.

The Contractor must adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect District Data in a manner that complies with New York, federal and local laws, rules and regulations and the District's policies. Education Law § 2-d requires that the Contractor provide the District with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable State, federal and local data security and privacy requirements. The Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C and is incorporated into this DPA.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

5. The District's Data Security and Privacy Policy

State law and regulation requires the District to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. The Contractor represents and warrants that it will comply with the District's data security and privacy policy and other applicable policies.

6. Right of Review and Audit.

Upon request by the District, the Contractor will provide the District with copies of its policies and related procedures that pertain to the protection of PII and District Data. The policies and procedures may be made available in a manner that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required by the District to undergo an audit of Contractor's privacy and security safeguards, measures and controls as they pertain to alignment with the requirements of applicable New York, federal and local laws, rules and regulations, the District policies applicable to the Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at the Contractor's expense, and provide the written audit report to the District. The Contractor may provide the District with a recent industry standard audit report performed by an independent third party on the Contractor's privacy and security practices as an alternative to undergoing an audit. The determination of whether the previously prepared audit report is "recent" will be determined by the District in its sole judgment.

7. Access to/Disclosure of District Data

(a) The Contractor agrees that it will limit the Contractor's internal access to and only Disclose PII to the Contractor's officers, employees and Subcontractors who need to access the PII in order to provide the Services and that the disclosure of PII will be limited to the extent necessary to provide the Services pursuant to the Service Agreement. The Contractor must take all actions necessary to ensure that all its officers, employees and Subcontractors comply with the terms of this DPA.

(b) The Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to District Data must be contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) The Contractor must examine the data security and privacy measures of its Subcontractors prior to utilizing the Subcontractor to ensure compliance with this DPA. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, the Contractor must: notify the District and prevent the Subcontractor's continued access to District Data; and, as applicable, retrieve all District Data received or stored by Subcontractor and/or ensure that District Data has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, the Contractor must follow the Data Breach reporting requirements set forth herein.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

(d) The Contractor will take full responsibility for the acts and omissions of its officers, employees and Subcontractors.

(e) The Contractor must not Disclose District Data to any other party (a party other than the Contractor's officers or employees or Subcontractors who does not need access to the District Data to provide the Services pursuant to the Service Agreement) without the prior written consent of the District (if necessary, the District will obtain the required consent(s) from third parties) unless the disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the District of the court order or subpoena in advance of compliance but in any case, provides notice to the District no later than the time the District Data is disclosed, unless such disclosure to the District is expressly prohibited by the statute, court order or subpoena.

(f) Except as prohibited by law, the Contractor will: (i) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking District Data; (ii) consult with the District regarding the Contractor's response; (iii) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and (iv) upon the District's request, provide the District with a copy of the Contractor's response.

(g) Upon the District's request, the Contractor agrees that it will promptly make any District Data held by the Contractor available to the District.

8. Training.

The Contactor must ensure that all its officers, employees and Subcontractors who have access to PII have received or will receive training on the federal and State laws governing confidentiality of the data prior to receiving access.

9. Term and Termination.

This DPA will be effective as of the date the Service Agreement is effective and will terminate on the termination of the Service Agreement. However, the obligations of the parties pursuant to this DPA will survive the expiration of the Service Agreement and will continue until the Contractor and Subcontractors no longer retain PII and no longer retain access to PII.

10. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the District, and the Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the District, unless such retention is expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, expressly requested by the District for purposes of facilitating the transfer of PII to the District or expressly required by law. As applicable, upon expiration or termination of

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

the Service Agreement, the Contractor will transfer PII, in a format agreed to by the Parties to the District.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the District's written election to do so, the Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by the Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, or electronic imaging of hard copies) as well as any and all PII maintained on behalf of the Contractor in a secure data center and/or in cloud-based facilities that remain in the possession of the Contractor or its Subcontractors, the Contractor will ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) The Contractor will provide the District with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that the Contractor and/or its Subcontractors continue to be in possession of any de-identified data (*i.e.,* data that has had all direct and indirect identifiers removed), the Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

11. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or Disclose PII for a Commercial or Marketing Purpose.

12. Encryption.

The Contractor will use industry standard security measures including Encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must Encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

13. Storage.

Contractor must store all District Data within the United States of America.

14. Breach.

a. The Contractor must promptly notify the District of any Breach of PII in the most expedient way possible and without unreasonable delay and in no event more than seven calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing and by email (if email address is provided) and personal delivery or nationally recognized overnight carrier. Notifications must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

representatives who can assist the District. Violations of the requirement to notify the District are subject to civil penalty(ies) pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law §2-d may subject the Contractor to additional penalties.

b. Notifications required to be made to the District pursuant to this paragraph must be sent to the following people at the following addresses:

Dr. Jordan Cox
Superintendent of Schools
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: jcox@commack.k12.ny.us

Mrs. Alise Pulliam
Executive Director for Instructional Technology
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: apulliam@commack.k12.ny.us

15. Cooperation with Investigations.

Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' officers, employees or Subcontractors, as related to such investigations, will be the sole responsibility of the Contractor if the Breach is attributable to Contractor or its Subcontractors.

16. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor will pay for or promptly reimburse the District for the full cost of the District's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law § 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the District. To the extent Student Data is held by the Contractor pursuant to the Service Agreement, the Contractor must respond within 20 calendar days to the District's requests for access to Student Data so the District can facilitate review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by the Contractor pursuant to the Service Agreement, the Contractor must promptly notify the District and refer the Parent or Eligible Student to the District.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

2. Bill of Rights for Data Privacy and Security.

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are annexed hereto as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The Contractor must complete and sign Exhibits A and B. Pursuant to Education Law § 2-d, the District is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA will govern and prevail, will survive the termination of the Service Agreement in the manner set forth herein, and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which will be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto will be and constitute an original signature, as if all parties had executed a single original document.

Commack Union Free School District	
By: (Signature) DocuSigned by: Alise Pulliam 736E7C729E52437...	By: (Signature) DocuSigned by: Jason Slater 10C2B3D5B8E54D0...
Alise Pulliam	(Printed Name) Jason Slater
Executive Director for Instructional Technology	(Title) IT Director
Date: 6/30/2023	Date: 6/30/2023

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

EXHIBIT A - Education Law § 2-d Parents' Bill of Rights for Data Privacy and Security

COMMACK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY –

Summary of Rights and Information for Parents and Students

The legislature and governor passed a group of bills that adjusted the Regents Education Reform Agenda. These bills are known collectively as the "Common Core Implementation Reform Act." One of the key components of this act (Chapter 56, Part AA, Subpart L, of the laws of 2014) directs the Commissioner of Education to appoint a Chief Privacy Officer (CPO). A major function of this new position is to work with school districts and parents to develop elements for a parents' bill of rights to help ensure that student data is private and secure. The State Education Department (SED) and the CPO must also recommend regulations to establish standards for data security and privacy policies that will be implemented statewide.

SED has issued a preliminary Parents' Bill of Rights for Data Privacy and Security. The Commack Union Free School District is issuing this summary of parents' rights under the new law. While some additional elements will be developed in conjunction with the CPO, districts, parents and the Board of Regents, this summary sets forth the key rights and information that parents should be aware of in regards to ensuring the privacy and security of their student's educational data.

The Commack Union Free School District is committed to ensuring student privacy and recognizes that parents, legal guardians, and persons with a parental relationship to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. To this end, the District is providing the following Parent's Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record;

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

writing to the Office of Information & Reporting Services, New York State Education Department, Room 863, 89 Washington Avenue, New York 12234; and

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to Alise Pulliam, Executive Director for Instructional Technology, PO Box 150, Commack, New York 11725, Phone: (631) 912-2027, Email: alisepulliam@commack.k12.ny.us or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

If the Commack Union Free School District enters into a third-party contract in which the service provider receives student data or teacher or principal data in order to provide a needed service for the District, supplemental information shall be developed and provided to parents that states:

6. The exclusive purposes for which the student data or teacher or principal date will be used;

7. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

8. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

9. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

10. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The CPO as appointed by the Commissioner must secure input from parents and other education and expert stakeholders to develop additional elements for the Parents' Bill of Rights for Data Privacy and Security. The Commissioner of Education will also be promulgating regulations with a comment period for parents and other members of the public to submit comments and suggestions to the CPO.

In the meantime, you can access additional information and a question and answer document issued by SED as a preliminary Parents' Bill of Rights for Data Privacy and Security.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

If you have any further questions or concerns at this time, please contact Dr. Jordan Cox, Superintendent, Commack UFSD, PO Box 150, Commack, New York 11725 or Mrs. Alise Pulliam at apulliam@commack.k12.ny.us

By: (Signature) DocuSigned by: Jason Slater
(Printed Name) Jason Slater
(Title) IT Director
Date: 6/30/2023

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors ("Service Agreements") that will receive Personally Identifiable Information ("PII") from Student Data or Teacher or Principal APPR Data.

Term of Service Agreement	Agreement Start Date: July 1st, 2023 Agreement End Date: June 30th, 2026
Description of the purpose(s) for which Contractor will receive/access/use PII	PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District. List Purposes: OUr company operates an elementary skill practice website where data is used solely for login and activity tracking and completing purposes.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☒ Teacher or Principal APPR Data
Subcontractor Written Agreement Requirement	The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Service Agreement. Check applicable option. ☐ Contractor will not utilize Subcontractors.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

	☒ Contractor will utilize Subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
Challenges to Data Accuracy	Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District's written request.
Secure Storage and Data Security	The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data: (a) Storage of Electronic Data (check all that apply): ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

	☐ Other: (b) Storage of Non-Electronic Data: Any data on paper is kept in our secure office building where access is limited. (c)Personnel/Workforce Security Measures: All employees are vetted, background checked, and must attend annual data privacy and data security training. (d) Account Management and Access Control: Only employees with job-related requirements can access PII data. (e) Physical Security Measures: Locked office building; locked desk drawers; locked and 2FA enabled office computers, secure local server room. (f) Other Security Measures: n/a
Encryption	Data will be encrypted while in motion and at rest.

By: (Signature)	DocuSigned by: Jason Slater
(Printed Name)	Jason Slater
(Title)	IT Director
Date:	6/30/2023

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Commack Union Free School District is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. The Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. The terms of the plan cannot conflict with any other terms of or Exhibits to the Data Privacy Agreement to which this Exhibit C is attached. **While this plan is not required to be posted to the District's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems. DO NOT LIMIT RESPONSES TO THE SPACES PROVIDED.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract	TPW maintains clear and concise data security policies and procedures and reviews and updates each annually.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	PII is protected via a user access rights control as well as full encryption while in transit and at rest.
3	Specify how your officers, employees and Subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and State laws that govern the confidentiality of PII.	All associates must complete mandatory data privacy training annually and sign off to verify completion.
4	Outline the processes that ensure that your officers, employees and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	Associates must pass background checks, be vetted, and also attend both data privacy training and general security training annually.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the District.	Any data security, privacy, or breach incidents will be identified, secured, and fully reported to an affected district within 5 days of knowledge of the incident. TPW maintains log files, access files, and runs a host of programs to secure networks and data.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	Any pertinent data will be transmitted to the district via secure files online if necessary.
7	Describe your secure destruction practices and how certification will be provided to the District.	PII is destroyed after 90 days of account inactivity or at any time upon a request from the district. Verification is provided in writing via email.
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	TPW's data security and privacy practices strive to protect all PII using the same safe methods that the district uses and requires.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	***YOU MAY USE TEMPLATE BELOW***

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	IknowIt.com assigns roles and controls to mandate data privacy to mitigate risk.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions	Roles and responsibilier in the business environment are defined and decisions are made in a manner to protect data security and integrity.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	All personnel are to inform management of any perceived security risk immediately.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	The organization understands the risk.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The organization supports operation risk decisions based on established requirements.

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	IknotIt.com has implemented processes to identify and mitigate supply chain risks.
PROJECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Access to physical and logical assets is limited in access to associated with required access.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Annual cybersecurity and data privacy training is attended by all personnel.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Information confidentialiyy, integrity, and availability are protected via our risk strategy assessment and policies.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Security policies and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	All systems, hardward, and software components are kept up to date.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Technical security solutions are managed and ensure the security and resilience of systems and assets according to our policies.
	Anomalies and Events (DE.AE):	Technical security solutions are managed and

DocuSign Envelope ID: BD9CF576-A67C-4F63-9D13-B63355309BE1

DETECT (DE)	Anomalous activity is detected and the potential impact of events is understood.	ensure the security and resilience of systems and assets according to policies.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Systems are tested regularly using both internal and external resources.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Intrusion detection processes are in place and run regularly.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Response plans are established and updated to handle any incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	If and when necessary: coordination with appropriate law enforcement agencies would take place.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Processes are analyzed to ensure proper response and recovery.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Disaster migitation is used to minimize negative effects of any cybersecurity event.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We build on our established processes by improving and enhancing.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery processes and procedures are executed in a timely manner.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	We build on our established processes by improving and enhancing.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Restoration activities are coordinated with all appropriate parties as needed.