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 SchoolPay ("the Contractor"), that is being entered into for a Three year term for the use of _SchoolPay 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.

I. 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 PU 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 "PU" 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 the Contractor's obligations pursuant to the Agreement and for no other purpose.

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.

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:

SchoolPay

Rick Killian
40 Burton Hills Blvd
Suite 415
Nashville, TN

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

With a copy to:
Bond, Schoeneck, & King 68
South Service Road, Suite 400,
Melville, NY 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 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: _____

Alise Pulliam
Executive Director for Innovation and Technology

SchoolPay
_____, **the Contractor**

By: _____

Name: Hume Miller
Title: CEO Education

EXHIBIT A

DATA PRIVACY AGREEMENT

COMMACK UNION FREE SCHOOL DISTRICT DATA PRIVACY AGREEMENT

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

SchoolPay

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and SchoolPay ("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.

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 June 16th, 2025.

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.

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,s 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.

5. The District's Data Security and Privacy Policy

State law and regulation require 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 the 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.

(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 Contractor 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 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 Pll 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 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 Pll affected and the number of records affected; a description of Contractor's investigation; and the contact information for

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.kl2.ny.us

Mrs. Alise Pulliam
Executive Director for Innovation and 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.

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)	By: (Signature)
Alise Pulliam	(Printed Name) Hume Miller
Executive Director for Innovation and Technology	(Title) CEO Education
Date:	Date:

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 (SEO) 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 Parents' 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 writing to the Office of Information & Reporting Services, New York State Education Department, Room 863, 89 Washington Avenue, New York 12234

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: apulliam@commack.kl2.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 data 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 he 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.

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.kl2.ny.us.

SchoolPay
By: (Signature)
(Printed Name) Rume Miller
(Title) CEO Education
Date:

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.

SchoolPay	
Term of Service Agreement	Agreement Start Date: March 31st, 2026 Agreement End Date: June 30th, 2029
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: Allow students to pay school fines, and lunch
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PH □ 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. □ 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 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.

	D Other: (b) Storage of Non-Electronic Data: SchoolPay does not store District PII in non-electronic (paper) form. All District Data is maintained electronically within the PaySchools cloud-hosted environment on Amazon Web Services (AWS). Company policy prohibits confidential information from being stored on paper media, printed documents, or removable physical media. In the event any non-electronic data were to be generated incidentally, the Data Storage and Destruction Policy requires that hard-copy media be shredded or physically destroyed such that PII cannot be read or reconstructed, and Certificates of Destruction (CoDs) are obtained to verify successful disposal. (c) Personnel/Workforce Security Measures: Pre-employment background screening checks are conducted for all candidates commensurate with their position and level. All new employees complete a formal onboarding process and are required to acknowledge the Employee Handbook, Code of Conduct, Insider Trading Policy, and Restrictive Covenant Agreement. Employees are bound by a Mutual Confidentiality and Non-Disclosure Agreement. Security awareness training is mandatory upon hire (within 45 days) and annually thereafter, delivered through KnowBe4. Training covers information security policies, data protection, social engineering/phishing, mobile device security, and acceptable use of technology. Random phishing awareness campaigns are conducted throughout the year. Developers receive additional annual training on secure software design and coding techniques. Failure to complete required training results in denial of access to company systems. Upon termination, employees must return all company-owned equipment, and all physical access mechanisms are returned or disabled. Accounts are updated weekly against HR census data, with separated employees disabled automatically.

	(d) Account Management and Access Control: Access is governed by a formal Access Control and Password Policy enforcing role-based access controls (RBAC) and least-privilege principles. Access is assigned on a need-to-know basis per the user's job role. Multi-factor authentication (MFA) is enforced for all users via Microsoft Entra ID and JumpCloud. The root account is disabled for operational use and blocked during provisioning. Password standards require minimum 8 characters with numeric and alphabetic characters, a history of 4 previous passwords, and global/custom banned password lists. Passwords must be changed immediately upon first use and may not be shared. User accounts are updated weekly against HR census data, with separated employees disabled automatically. Quarterly management reviews of user access provide documented approval of role-specific reviews for all platforms. Backup modification rights are restricted through Infrastructure as Code policies. User identity and group membership are centrally managed through JumpCloud and Active Directory. (e) Physical Security Measures: The production environment is hosted on Amazon Web Services (AWS) in the US East (N. Virginia) region, leveraging AWS's world-class physical data center security. Critical components are replicated across multiple geographically separated availability zones. For corporate facilities, the organization implements facility entry controls to limit and monitor physical access to systems. Video cameras monitor access to all entry points to sensitive areas, with footage reviewed periodically and retained for at least 90 days. Sign-in logs are accessible for at least 90 days. Badges are used to distinguish between company personnel and visitors. Public access to network jacks is restricted. Physical access to wireless access points, gateways, networking hardware, and telecommunications lines is controlled. Consoles with direct access to servers housing sensitive data are locked when not in use and physically restricted from unauthorized personnel. Upon termination, all physical access mechanisms (keys, access cards) must be returned or disabled. (f) Other Security Measures:

	Encryption: All data at rest is encrypted across AWS services (EC2, S3, RDS, Aurora) using AWS KMS with cloud-provider and customer-managed keys. Data in transit is protected via HTTPS TLS 1.2. Removable storage must be encrypted with AES-256. Full disk encryption is required on all laptops. Vulnerability Management: Production networks undergo quarterly vulnerability scans. Annual third-party penetration tests are conducted. Source code vulnerability scans are performed as part of the SDLC. Critical and high issues are remediated and re-tested. Monitoring and Detection: 24/7 intrusion detection with third-party SOC monitoring by Blue Voyant. Security logs collected continuously with 365-day retention. Microsoft Sentinel provides centralized SIEM and DLP alert triage. Microsoft Defender for Cloud is enabled on every account. Endpoint Protection: Laptops centrally managed with hard-disk encryption, automatic patching, password enforcement, auto screen-lock, and remote wipe. Data Loss Prevention: DLP system classifies regulated, confidential, and business-critical data, identifies policy violations, and alerts administrators. Network Security: Multi-layered controls including VPC isolation, security groups, ACLs, Cloudflare WAF, VPN restrictions, and dev/staging/prod environment segregation.
Encryption	Data will be encrypted while in motion and at rest.

SchoolPay	
By: (Signature)	
(Printed Name)	Name Miller
(Title)	CEO Education
Date:	

EXHIBIT C

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

Responses Based on SOC 2 Type II Audit Report

Contractor: SchoolPay (i3 Verticals, LLC — i3 Education Division)

District: Commack Union Free School District

Service Agreement Effective Date: June 16, 2025

Source Documentation: i3 Verticals SOC 2 Type II Report (Audit Period: April 1, 2025 – September 30, 2025)

This document provides SchoolPay's responses to the nine questions required by the Commack Union Free School District's Data Privacy Agreement (Exhibit C) and the NIST Cybersecurity Framework v1.1 alignment table (Exhibit C.1). All responses are substantiated by controls, tests, and findings documented in the i3 Verticals SOC 2 Type II report and supporting policy documentation.

Exhibit C — Data Privacy and Security Plan Responses

The following table addresses each question required by the Commack UFSD Data Privacy Agreement, Exhibit C.

#	Question	SchoolPay / i3 Verticals Response
1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	SchoolPay (operated by i3 Verticals) maintains a comprehensive information security program governed by formally documented policies and procedures that are reviewed and approved by management on an annual basis. All 19 policy documents are maintained on a centralized OneDrive share and were last reviewed and approved within the past 12 months. The program is aligned with SOC 2 Type II trust services criteria (Security, Availability, and Confidentiality) and PCI DSS requirements, and the company undergoes annual independent third-party audits to validate the implementation and operating effectiveness of its control environment. Throughout the contract term, SchoolPay will continue to: enforce role-based access controls and least privilege principles; encrypt all PII at rest and in transit; conduct annual risk assessments; perform quarterly vulnerability scans and annual penetration tests; maintain security awareness training for all personnel; and update policies to reflect evolving regulatory requirements, including FERPA, COPPA, NY Education Law §2-d, and 8 NYCRR Part 121. Management convenes monthly with a fixed agenda to oversee objectives, evaluate risks and threats, and discuss security, availability, and confidentiality non-compliance issues, ensuring continuous governance throughout the contract lifecycle.
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	Administrative Safeguards: Formal Information Security Policy reviewed annually; documented job descriptions defining security responsibilities; pre-employment background screening; Employee Handbook and Code of Conduct acknowledgment upon hire; quarterly management access reviews; and a designated CISO and Director of Cybersecurity overseeing the security program. Operational Safeguards: Annual risk assessments using a formal risk control matrix (RCM); third-party vendor risk management program with annual security assessments; Data Loss Prevention (DLP) system classifying regulated, confidential, and business-critical data with alerts sent to administrators; centrally managed endpoint protection with hard-disk encryption, automatic patching, password enforcement, auto screen-lock, and remote wipe capabilities; and a Security and Privacy Incident Response Plan (SPIRT) with defined roles for Security, IT, and Compliance. Technical Safeguards: All data encrypted at rest using AWS KMS (EC2, S3, RDS, Aurora instances) and in transit using HTTPS TLS 1.2; multi-factor authentication (MFA) enforced for all 311 users via Microsoft Entra ID and JumpCloud; role-based access controls with quarterly reviews; network segmentation with VPC isolation, security groups, ACLs, and Cloudflare WAF; intrusion detection

		systems scanning 24/7 with third-party monitoring by Blue Voyant; Microsoft Defender for Cloud automated across every account; and audit trail generation retained for 365 days.
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 employees are required to complete security awareness training upon hire (within 45 days) and annually thereafter. Training is delivered through the KnowBe4 learning management system (LMS) and covers information security policies, standards, responsibilities, acceptable use of end-user technologies, common security risks, information security and data protection, mobile device security, and social engineering/phishing awareness. Compliance-related training (including anti-harassment and ethics) is administered through UKG. Personnel are required to acknowledge that they have read and understood information security policies, including responsibilities for managing sensitive data. Additional specialized training includes: phishing awareness campaigns conducted randomly throughout the year by the IT team to test effectiveness; annual software security training for developers covering secure design, secure coding techniques, and vulnerability detection tools; and at the CISO's discretion, supplemental training in response to security incidents, new policies, or new technology adoption. Failure to complete required training can result in denial of access to company systems. The most recent audit verified training records for a sample of 17 of 167 new hires and 30 of 887 existing employees, confirming completion of required security awareness courses.
4	Outline the process that ensures your officers, employees, and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	All new employees complete a formal onboarding process that includes acknowledging the following policy documents: Employee Handbook, Code of Conduct, Insider Trading Policy, and Restrictive Covenant Agreement (RCA). The Employee Handbook covers employment practices, workplace conduct, compensation, benefits, safety, timekeeping, use of company property and IT resources, among other areas. All employees and personnel are bound by a Mutual Confidentiality and Non-Disclosure Agreement that outlines handling of confidential business information, defines confidential information broadly, and lasts for two years with trade secret protections extending as long as the information qualifies under applicable law. For third-party contractors and subcontractors, the company's Third Party Risk Management Policy requires that contracts include provisions addressing information security, confidentiality, and privacy. Third-party engagements undergo contract review by Legal to ensure terms are appropriate for the organization's risk tolerance. Access to systems and data is revoked upon termination of any third-party relationship. Vendors are subject to information security,

		confidentiality, and privacy commitments as part of their agreements, and confidentiality commitments are reviewed at contract creation or renewal.
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.	SchoolPay maintains a formal Security and Privacy Incident Response Plan (dated August 2025) that outlines a structured approach for identifying, responding to, and resolving security and privacy incidents. The plan assigns clear roles to the Security and Privacy Incident Response Team (SPIRT), which includes representatives from Security, IT, and Compliance. Detection Capabilities: An intrusion detection system scans 24/7 for potential security issues via a third-party security operations center (Blue Voyant); security logs are continuously collected in the production environment with 365-day retention; alerts are triggered by predefined thresholds or anomalies; a DLP system classifies and monitors regulated data with automated alerts; and production networks undergo quarterly vulnerability scans. Incident Management Process: Incidents are categorized by severity and type; response actions are tracked using standardized worksheets and reports in Jira Service Desk; a root cause analysis is prepared and reviewed by management for high-severity incidents; change requests are prepared based on root cause analysis for remediation; and post-incident reviews assess damage, update policies, and document lessons learned. Reporting to the District: SchoolPay will notify the District of any breach of PII in the most expedient way possible and in no event more than seven calendar days after discovery, in compliance with Education Law §2-d. Notifications will include a description of the breach, types and number of PII records affected, a description of the investigation, and contact information for representatives who can assist the District.
6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of the Service Agreement, SchoolPay will, as directed by the District in writing, securely transfer all District Data in a format agreed to by the parties. The school district may also exercise a read-only option for a period of time prior to the site being completely shut down. SchoolPay stores sensitive data in databases labeled by customer and type, supporting organized and efficient data retrieval and transfer. The PaySchools Data Retention Policy (dated May 2025) defines retention periods ranging from three months to seven years as determined by data classification, ensuring data is available for transfer throughout the applicable retention period. Once the transfer has been accomplished, SchoolPay will proceed with secure destruction of all remaining District Data in accordance with the data destruction procedures described below.
7	Describe your secure destruction practices and how certification will be provided to the District.	SchoolPay maintains a formal Data Storage and Destruction Policy that governs the secure disposal

		of all data. Customer, client, and employee data must be destroyed when no longer useful to the business, and data destruction must not conflict with retention requirements or ongoing legal obligations. Certificates of Destruction (CoDs) are obtained to verify that confidential data stored on hard drives, tapes, SSDs, or other storage media was successfully destroyed. CoDs guarantee that data is destroyed with due diligence and cannot be recovered even using advanced forensic techniques. Each CoD must include: unique digital identifiers; model and serial numbers of storage devices disposed of; details of the sanitization method used; details of the verification method used; name of the software used for media sanitization; name of the technician performing data destruction; signature of the official verifying the disposal process; and start date/time of the sanitization process. For electronic data, automated deletion processes are tested at least quarterly, and any manual deletion follows documented change management oversight. A written certification of secure deletion and/or destruction will be provided to the District upon completion.
hj8	Outline how your data security and privacy program/practices align with the District's applicable policies.	SchoolPay's security program is designed to align with district data security and privacy policies that comply with Part 121 of the Regulations of the Commissioner of Education and the NIST Cybersecurity Framework. Key areas of alignment include: Compliance: SchoolPay undergoes annual SOC 2 Type II audits and PCI DSS assessments, demonstrating adherence to industry-recognized security standards that meet or exceed typical district requirements. Data Protection: All PII is encrypted at rest and in transit; access is restricted on a need-to-know, role-based basis; multi-factor authentication is enforced enterprise-wide; and data classification policies define handling requirements for various sensitivity levels. Incident Response: The Security and Privacy Incident Response Plan provides for timely notification to the District consistent with Education Law §2-d requirements (within seven calendar days). Training: All personnel with access to PII receive security awareness training upon hire and annually, covering federal and state data privacy laws. Vendor Management: Third-party subcontractors are subject to contractual security and privacy obligations and ongoing risk assessments, consistent with district expectations for supply chain governance.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	See NIST CSF v1.1 alignment table on the following pages.

Exhibit C.1 — NIST Cybersecurity Framework v1.1 Alignment

The following table demonstrates how SchoolPay's data security and privacy program materially aligns with the NIST Cybersecurity Framework v1.1 across all five core functions.

Function	Category	SchoolPay / i3 Verticals Response
IDENTIFY (ID)	Asset Management (ID.AM)	SchoolPay maintains a comprehensive asset inventory for the PaySchools environment, including compute and storage resources, cloud-specific items such as KeyVault assets, and cloud performance metrics. The inventory is reviewed by the Senior Director of Cyber Security on an annual basis. Assets are classified by access type, data type, sensitivity, and criticality. Configuration standards are documented for Windows, Linux, Amazon RDS, and Amazon S3 environments.
	Business Environment (ID.BE)	The organization's mission, objectives, stakeholders, and activities are clearly defined and communicated through an internal knowledge base that includes service charters, on-call expectations, and operational resources. The Board of Directors comprises nine members, meets quarterly, and exercises oversight of internal control development and performance. Management convenes monthly to oversee objectives and evaluate risks.
	Governance (ID.GV)	SchoolPay maintains 19 formally documented policies and procedures on a centralized OneDrive share, all reviewed and approved within the past 12 months. The Information Security Policy is reviewed annually and updated to reflect major changes. Executive management is responsible for evaluating and accepting risk, identifying security responsibilities and goals, and supporting legal and regulatory requirements. The company complies with SOX, PCI DSS, and undergoes annual SOC audits.
	Risk Assessment (ID.RA)	Annually and upon significant changes, the organization performs a formal risk assessment to identify critical assets, threats, and vulnerabilities. The result is formally documented in a risk control matrix (RCM) that is updated annually. Key stakeholders evaluate risks during an annual risk assessment meeting. The process includes instructions on risk management strategies: accept, avoid, limit, or transfer.
	Risk Management Strategy (ID.RM)	Risk treatment options include acceptance, avoidance, mitigation, and transfer. The formal RCM captures the organization's priorities, constraints, and risk tolerances. Management considers risk mitigation through cost-benefit analysis and identifies necessary control activities to support operational risk decisions.
	Supply Chain Risk Management (ID.SC)	The Third Party Risk Management Policy defines responsibilities for selection, engagement,

		management, and oversight of third-party relationships. The Vendor Risk Management program uses a Three Lines of Defense model. Third parties are assessed based on nature of services, data access, business impact, and contractual commitments. Criticality determines monitoring frequency: annual for Strategic vendors, biennial for Operational/Preferred, and triennial for Commodity-level vendors. Critical vendors' SOC 2 reports are reviewed annually.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	Access is restricted based on job responsibilities using role-based access controls and least privilege principles. MFA is enforced for all 311 users via Microsoft Entra ID and JumpCloud. The root account is disabled for operational use. Quarterly management reviews of user access are conducted, with automated weekly updates against HR census data. Accounts for separated employees are disabled in coordination with managers and HR. Password standards require minimum 8 characters with numeric and alphabetic characters, history of 4 previous passwords, and global banned password lists.
	Awareness and Training (PR.AT)	Security awareness training is mandatory upon hire (within 45 days) and annually thereafter, delivered via KnowBe4. Training covers policies, standards, data protection, mobile device security, and social engineering/phishing. Random phishing awareness campaigns test effectiveness throughout the year. Developers receive annual training on secure software design and coding techniques. Failure to complete training results in denial of system access.
	Data Security (PR.DS)	Data at rest is encrypted across all AWS services (EC2, S3, RDS, Aurora) using AWS KMS. Data in transit is protected via HTTPS TLS 1.2 authenticated certificates. Encryption keys are securely managed with access restricted to custodians with a business need. A DLP system classifies regulated, confidential, and business-critical data and monitors for policy violations. PANs are never transmitted via email, instant messaging, chat, or SMS. Removable storage devices must be encrypted using strong encryption algorithms such as AES-256.
	Information Protection Processes and Procedures (PR.IP)	Change management follows a structured process with Standard, Normal, and Emergency change types. Code changes require peer review, pull request checks, QA sign-off, and CAB approval prior to production deployment. The SDLC integrates security reviews addressing authentication, authorization, encryption, logging, and sensitive data handling. Static analysis and vulnerability scanning are performed on code modifications, with attention to third-party libraries and secure coding practices.
	Maintenance (PR.MA)	Centrally managed configuration management uses

		infrastructure-as-code with predefined configurations enforced on servers. Patch management processes cover laptops and servers. Infrastructure configurations are documented in formal Configuration Standards for Network and Infrastructure, covering AWS services, security group rules, DNS management, subnet architecture, and deployment pipelines through Azure DevOps.
	Protective Technology (PR.PT)	Network security controls include ACLs, security groups, Cloudflare WAF, access restriction per environment, and VPN restrictions. Microsoft Defender for Cloud is automated and enabled on every account. The multi-layered security model encompasses application-layer controls (MFA, unique IDs, complex passwords, IP source restriction, data encryption) and network/infrastructure controls (network architecture, vulnerability scanning, IDS/IPS). Audit trails are retained for 365 days.
DETECT (DE)	Anomalies and Events (DE.AE)	PaySchools operates a layered monitoring setup combining audit trails, availability tracking, and alerting mechanisms. Alerts are triggered by predefined thresholds or anomalies and routed to appropriate stakeholders. Notifications are categorized by urgency, with higher-priority incidents investigated promptly. The third-party security operations center (Blue Voyant) provides 24/7 monitoring and incident rating.
	Security Continuous Monitoring (DE.CM)	Security logs are continuously collected in the production environment to capture user actions and cloud service activities, with retention configured for 365 days. Production networks undergo quarterly vulnerability scans. An intrusion detection system scans 24/7 for potential security issues. Endpoint protection is centrally managed with regular updates. Microsoft Sentinel provides centralized log management and DLP alert triage.
	Detection Processes (DE.DP)	The Vulnerability Management Policy requires penetration testing of internal networks, external networks, and hosted applications at least semi-annually. Identified vulnerabilities must be corrected and re-tested. Annual third-party penetration tests are conducted (most recently in January 2025, a gray-box test of the i3 Education application). File integrity monitoring and change detection software are used on logs and critical files to alert personnel to unauthorized modifications.
RESPOND (RS)	Response Planning (RS.RP)	The Security and Privacy Incident Response Plan (dated August 2025) provides a structured approach for identifying, responding to, and resolving incidents. The SPIRT includes representatives from Security, IT, and Compliance. Incidents are categorized by severity and type. Response actions are tracked using standardized worksheets and reports in Jira Service Desk. The

		plan is maintained and updated to reflect emerging risks and lessons learned.
	Communications (RS.CO)	Detected incidents are communicated and reviewed by the individual responsible for security management. The incident response process includes documented escalation protocols and communication tools. External stakeholders, including affected districts, law enforcement, and relevant parties, are notified as required by applicable laws and regulations. The disaster recovery exercise identified improvements for defined communication channels and backup alerting processes.
	Analysis (RS.AN)	A root cause analysis is prepared and reviewed by management for high-severity incidents. Change requests are prepared based on the root cause analysis to drive remediation and resolution. Post-incident reviews assess damage, update policies, and document lessons learned. The incident response handling is verified against the formal plan to ensure alignment with documented procedures.
	Mitigation (RS.MI)	Incident response activities include containment, investigation, and documentation. Backup systems are restored as part of remediation efforts, which may include reinstalling affected systems and recovering data from backups. Vulnerability remediation follows defined standards, with critical and high issues investigated and resolved with retesting to confirm correction. The company maintains a monitoring program for continual assessment of the control environment.
	Improvements (RS.IM)	Post-incident reviews are required to assess damage, update policies, and document lessons learned from current and previous detection/response activities. Contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents.
RECOVER (RC)	Recovery Planning (RC.RP)	A documented Business Continuity and Disaster Recovery Management Plan outlines the approach for maintaining operations during and after disruptive events, reviewed annually (last approved June 2025). It includes a lifecycle framework covering risk assessment, BIA, recovery strategies, plan development, and regular testing. Backup policies cover daily, weekly, and monthly snapshots with cross-region replication. Recovery objectives target restoring applications within 30 minutes and databases within 3 hours. The DR plan is tested at least annually.
	Improvements (RC.IM)	The most recent DR exercise identified areas for improvement, including defined communication channels, backup alerting processes, and visibility into business-driven restoration priorities. Testing plans and post-mortems capture results and lessons learned, feeding into continuous

		improvement of the disaster recovery approach.
	Communications (RC.CO)	Recovery exercises coordinate communication plans, fail-over scenarios, and operational transitions across teams. Site24x7 and Jira Operations provide monitoring and alerting within minutes of an incident. Customers are notified of service interruptions based on the Service Level Agreement. The recovery process emphasizes coordination among emergency teams and remote work capabilities to sustain critical functions during prolonged disruptions.