



SERVICES AND DATA PRIVACY AGREEMENT

Phoenix Central School District
and

SmartPass, Inc.

This Data Privacy Agreement ("DPA") is by and between the Phoenix Central School District ("EA"), an Educational Agency, and SmartPass, Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of 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:** means 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. 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.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.

6. **Eligible Student:** A student who is eighteen years of age or older.
7. **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.
8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **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.
11. **Release:** Shall have the same meaning as Disclose.
12. **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.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **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.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **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 under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 12/13/2024 ("Service Agreement"); Contractor may receive PII regulated by several New York

and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (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 Section 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. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA 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. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA 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. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA.

Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is 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) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and 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 EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall 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) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that 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), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

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

11. Encryption.

Contractor shall 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.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and 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 representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: Michael Foley

Title: Data Privacy Officer

Address: 116 Volney Street

City, State, Zip: Phoenix, NY 13135

Email: mfoley@phoenicsd.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA 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' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

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

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 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 EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such 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 Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA 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 shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede 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 shall 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 shall be and constitute an original signature, as if all parties had executed a single original document.

| EDUCATIONAL AGENCY | CONTRACTOR |
|---------------------------------|---------------------------------|
| BY: <i>Christopher J. Byrne</i> | BY: <i>Mary Anne Laracochea</i> |
| Christopher Byrne | Mary Anne Laracochea |
| Superintendent | VP of Operations |
| Date: 2024-12-16 | Date: 12/16/2024 |

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: Michael Foley, Data Privacy Officer, 116 Volney Street, Phoenix, NY 13135, mfoley@phoenixcsd.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

| CONTRACTOR | |
|----------------|----------------------|
| [Signature] | Mary Anne Laracochea |
| [Printed Name] | Mary Anne Laracochea |
| [Title] | VP of Operations |
| Date: | 12/16/2024 |

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 Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

| | |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name of Contractor | SmartPass Inc. |
| Description of the purpose(s) for which Contractor will receive/access PII | SmartPass is a web-based digital hall pass system that replaces traditional sign-out books, paper passes, and wooden blocks. It allows you to have complete oversight on how your students travel through your hallways during class time. |
| Type of PII that Contractor will receive/access | Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data |
| Contract Term | Contract Start Date <u>Subscription date based on quote</u> Contract End Date <u>Subscription date based on quote</u> |
| Subcontractor Written Agreement Requirement | Contractor will not utilize subcontractors without a written contract that requires 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 Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors. |
| Data Transition and Secure Destruction | Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. Securely delete and destroy data. |
| Challenges to Data Accuracy | Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request. |

| | |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Storage and Data Security | <p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>SmartPass maintains a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.</p> |
| Encryption | <p>Data will be encrypted while in motion and at rest.</p> |

| CONTRACTOR | |
|-----------------------|-----------------------------|
| [Signature] | <i>Mary Anne Laracochea</i> |
| [Printed Name] | Mary Anne Laracochea |
| [Title] | VP of Operations |
| Date: | 12/16/2024 |

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) 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. For every contract, 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. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

| | | |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract. | SmartPass will not use any information in a student record for any purpose other than those required or specifically permitted by the SmartPass Terms of Use and Privacy Policy Statement. |
| 2 | Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. | Data is stored in Google Cloud only within the United States for as long as the school has an active subscription with us. You may also check SmartPass Terms of Service available at smartpass.app/terms and Privacy Policy available at smartpass.app/privacy . |
| 3 | Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII. | All of our employees go through comprehensive security awareness training, covering all the basics including: device security, privacy, social media, remote working, personal email, browsing internet securely, password security, and more. |
| 4 | Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum. | All of our employees go through comprehensive security awareness training, covering all the basics including: device security, privacy, social media, remote working, personal email, browsing internet securely, password security, and more. |
| 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 EA. | In case of data breach, the following occurs: The date and time the data breach was discovered is documented; The response team is notified; The location of the data breach is isolated; Additional data loss will be stopped; All possible data about the breach will be gathered; The investigation about the breach will be documented; Law enforcement will be notified; Customers will be notified; An in-depth investigation will be performed Customers will be notified within 7 business days via email. This primarily includes the specified district point of contacts. |
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | Data will be deleted within 1 year by default. A request must be sent in writing for a dump of protected data or to ask for an early deletion of data. |
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | Post-Contract Data Deletion: SmartPass hereby certifies that, upon the termination of a service contract with a School District, it shall isolate and permanently delete any and all Student Records belonging to such School District that may remain on the System, unless the School District or applicable regulations require the retention of such data, in which case the records shall be deleted upon the expiration of the retention period. |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | We comply with the following laws concerning the protection of student personally identifiable information, including educational records: 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"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C.1232h, AB 1584 (codified at California Education Code § 49073.1), and the Student Online Personal Information Protection Act (codified at California Business and Professions Code § 22584 et seq.) |
| 9 | Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below. | Reference: https://www.smartpass.app/privacy PLEASE USE TEMPLATE BELOW. |

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. | We maintain a detailed, manually updated inventory of all physical and digital assets, including hardware and software license keys. Currently, we lack a formal enterprise management software solution for managing these devices, instead opting for manual management. |
| | 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. | Our primary stakeholders are the schools that use our SaaS software. Our mission focuses on facilitating smarter movement and better learning outcomes. We aim to ensure the security of student data while providing valuable insights to schools to enhance learning outcomes. |
| | 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. | We follow the guidelines set out by NIST and consistently review the requirements in Data Processing Agreements (DPAs) and licensing agreements, adjusting our cybersecurity policies accordingly to maintain compliance. We also adhere to state and federal requirements such as COPPA and FERPA. |
| | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | We identify and assess cybersecurity risks during code reviews by consistently monitoring for security vulnerabilities. We've implemented guidelines for validating request parameters and checking access privileges. In terms of infrastructure, we use Google Cloud, which offers various security benefits over traditional self-managed infrastructure stacks, such as default disk encryption and SSL for secure communication. |
| | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | Our organization prioritizes risks based on their potential impact on our mission to provide secure, efficient educational technology. We have a formal process to evaluate and treat identified risks, which includes regular reviews and updates to our risk management approach in response to changes in our business environment or the wider threat landscape. Given our focus on student data security, we prioritize risks that could compromise data integrity and confidentiality. |
| | 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. | We prioritize managing supply chain risks based on their operational importance and data sensitivity. We uphold low risk tolerance due to the nature of student data we handle. Preliminary risk management includes due diligence of suppliers' security standards before onboarding. We ensure to work with reputable vendors and incorporate security clauses in contracts. If suppliers' practices are found inadequate, we address improvements or consider alternative suppliers. Our aim is ongoing enhancement of supply chain risk management practices. |

| Function | Category | Contractor Response |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PROTECT (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. | User identities are managed through rostering integrations, with authentication handled externally through our Single Sign-On integrations. Access to systems and data is controlled through Role- Based Access Control (RBAC) with different privilege tiers. All company accounts utilize enforced SMS 2FA authentication, and privileged accounts are managed by adding RBAC rules for specific usage rather than granting temporary privileges. |
| | 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. | We provide written documentation about common cybersecurity threats, including phishing attacks, specifically targeting startups. This comprehensive guidance is mandatory reading for all employees, ensuring a baseline understanding of potential threats and best practices for cybersecurity. |
| | 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. | Data is encrypted both at rest and in transit using industry-standard practices such as SSL. Data integrity is maintained through robust change management practices and regular data backups. |
| | 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. | We adhere to a defined set of rules for handling Personally Identifiable Information (PII), delineating where PII can be stored and displayed. These rules contribute to our overall procedures for protecting sensitive information. |
| | Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. | We employ automated updates and patching at all levels, from the hardware layer managed by Google Cloud to our operating system and control plane components. Software dependencies are monitored through automated vulnerability scanning. |
| | 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. | To protect our systems and data, we utilize multiple technologies including automated email spam filtering, two-factor authentication, network and application firewalls, and disk encryption. |
| DETECT (DE) | Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. | We actively monitor a range of metrics surrounding performance and data transfer, recognizing that abnormal data transfers and performance often indicate unusual activity. Our system is set up with automatic alarms tied to these metrics, which trigger alerts for our on-call team, ensuring round-the-clock monitoring every day of the year. |
| | Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | Our systems and data are continuously monitored for potential cybersecurity threats through automated alarms and a dedicated on-call rotation. This ensures that any potential threats or anomalies can be swiftly identified and addressed. |
| | Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. | We leverage automated alarms for detection and internally log and monitor metrics. Our detection capabilities are reviewed annually as part of our general security strategy review, ensuring our processes and systems are kept up-to-date with the latest security standards and threats. |

| Function | Category | Contractor Response |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RESPOND (RS) | Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | Upon detecting a cybersecurity incident, we activate our formal incident response plan. Immediate action is taken to mitigate the incident and work on a proper fix. This involves notifying relevant parties, including customers and authorities, and taking <u>steps to restore business function</u> . |
| | Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | Within our organization, we discuss cybersecurity incidents openly to learn from them and prevent future recurrence. For external communication, we provide full information about the cybersecurity incident to stakeholders and the public, maintaining transparency in our operations. |
| | Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities. | The impact of cybersecurity incidents is analyzed using our extensive network logging. We take a proactive approach to security, logging relevant data for later analysis and investigation. |
| | Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. | Upon detecting an incident, the affected systems are isolated to prevent further spread. A thorough investigation is initiated to understand the scope and nature of the breach, while our IT and security teams work on addressing vulnerabilities and <u>restoring systems</u> . These steps form part of our standard incident response plan. |
| | Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | Post-incident, we conduct a comprehensive review to identify improvement areas, including technical aspects, communication, decision-making, and coordination efforts. Lessons learned are used to update our cybersecurity practices and incident response plan, enhance team training, and are tested through regular drills and simulated attack exercises. |
| 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. | Our organization maintains a detailed recovery plan that outlines the steps for system, asset, and data recovery in the event of a cybersecurity incident. The plan includes restoring systems from secure backups, verifying recovered data integrity, and ensuring vulnerabilities are effectively addressed before systems are restored. |
| | Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. | After a cybersecurity incident, we carry out a comprehensive post-incident analysis to identify areas for improvement in our recovery strategies. This process includes examining the effectiveness of our response and recovery actions, the sufficiency of our backups, and the timeliness of our recovery. The lessons learned from this analysis are integrated into our recovery plan to boost our resilience against future incidents. |
| | 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). | Open and transparent communication is a crucial part of our recovery process. We keep our employees informed about the recovery progress and anticipated timelines. Additionally, we update our stakeholders on the incident, our recovery actions, and the measures we're implementing to avert similar incidents in the future. This maintains trust and showcases our commitment to cybersecurity. |

EXHIBIT D – JOINDER AGREEMENT

This Joinder Agreement (“Joinder”) is effective as of the date of signature below and is entered into by the undersigned Participating School pursuant to that certain Agreement, dated _____, 20____, by and between _____ and Phoenix Central School District (the “Agreement”). Capitalized terms used but not defined in this Joinder shall have the respective meanings ascribed to such terms in the Agreement. By the execution of this Joinder, the Participating School (i) agrees to be bound by, and subject to, the terms and conditions of the Agreement as a “Participating School” and a “Party” thereunder, (ii) adopts the Agreement with the same force and effect as if the Participating School was originally a party thereto, and (iii) agrees that any Confidential Data provided by the Participating School to Vendor shall be governed by the Agreement.

The Agreement shall extend only to the data privacy and security matters that are the subject matter thereof and the Terms shall continue to govern with respect to all other matters. In the event of a conflict or an inconsistency between the terms and conditions of the Terms and the terms and conditions of the Agreement, the Agreement shall govern and control.

In order for this Joinder to be effective, the Participating School must send a signed copy of this Joinder to Phoenix Central School District via email to mfoley@phoenixcsd.org or by mail to Michael Foley, Director of Data and Instructional Technology, Phoenix Central School District, 116 Volney Street, Phoenix, NY 13135 and to Vendor via email at **Vendor Email** or by mail to Attn: **Vendor Contact, Vendor Address**.

Name of Participating School: _____

By: _____

Name: _____

Title: _____

Date: _____

Address: _____

Audit trail

Details

FILE NAME ED Law 2D Agreement.pdf - 12/16/24, SmartPass

STATUS ● Signed

STATUS TIMESTAMP 2024/12/16
17:01:17 UTC

Activity


SENT

mfoley@phoenixcsd.org **sent** a signature request to:
• Christopher J. Byrne (cbyrne@phoenixcsd.org)

2024/12/16
16:52:37 UTC


SIGNED

Signed by Christopher J. Byrne (cbyrne@phoenixcsd.org)

2024/12/16
17:01:17 UTC


COMPLETED

This document has been signed by all signers and is **complete**

2024/12/16
17:01:17 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.