

DATA PRIVACY AGREEMENT

Schenectady City School District
and

Skills 21 at EdAdvance

This Data Privacy Agreement ("DPA") is by and between the Schenectady City School District ("EA"), an Educational Agency, and Skills21 at EdAdvance ("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 [5/7/25] ("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:
 - (i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or
 - (ii) 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: Kurt Redman

Title: Director of Instructional Technology

Address: Schenectady City School District 108 Education Drive

City, State, Zip: Schenectady, NY 12303

Email: redmank@schenectadyschools.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.

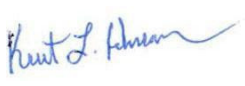
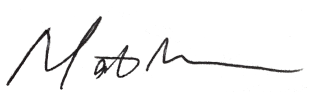
EDUCATIONAL AGENCY	CONTRACTOR
BY: <i>[Signature]</i> 	BY: 
<i>[Printed Name]</i> Kurt L. Redman	Matt Mervis
<i>[Title]</i> Data Privacy Officer	Skills21 Director
Date: 5/8/25	Date: 5/7/25

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

The Schenectady City School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information (PII) 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 PII, 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 the following website <http://www.nysed.gov/student-dataprivacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/studentdataprivacy/form/report-improper-disclosure>.

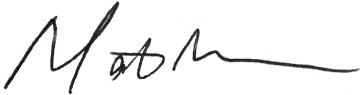
CONTRACTOR	
[Signature]	
[Printed Name]	Matt Mervis
[Title]	Director Skills21
Date:	5/7/25

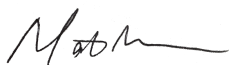
EXHIBIT B

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	Skills21 at EdAdvance
Description of the purpose(s) for which Contractor will receive/access PII	Beyond the Peaks Student Film Festival Platform
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 _____SY 2025-2026_____ Contract End Date _____SY 2025-2026_____
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	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <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	<p>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.</p>
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>Please see Skills21 Launchpad Privacy Statement</p> <p>https://microai.skills21.org/Skills21%20LP%20Privacy%20Statement%20and%20Contract.p df</p>
Encryption	<p>Data will be encrypted while in motion and at rest.</p>

CONTRACTOR	
[Signature]	
[Printed Name]	Matt Mervis
[Title]	Director Skills21

Date:	5.7.25
-------	--------

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.	<p>Skills21 Launchpad collects student data necessary to support educational activities, including name, email, gender, school, grade, and race. This data is used solely to create and manage student accounts, support challenge-based learning, fulfill grant reporting requirements (in aggregated and de-identified form), and for system performance analytics. All such uses are in accordance with the Student Data Privacy Act and FERPA regulations (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 4.a.i–iii – Use of Student Data).</p> <p>Student data is retained only as long as necessary or as required by legal obligations. Deletion requests from authorized individuals or districts will be honored unless prohibited by law or retention requirements related to disaster recovery systems. Districts retain ownership and control over student data, and students or their guardians may request corrections or deletions at any time (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.i–iii – Retention of Student Data).</p> <p>Skills21 implements a secure web-based storage system with multiple layers of protection to safeguard data from unauthorized access. These measures are aligned with state and federal standards. Additionally, while artificial intelligence tools like OpenAI's ChatGPT API may be used, they do not contribute to AI model training and remain governed by privacy laws (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>In the event of a data breach, Skills21 will notify affected school districts within 48 hours and provide a detailed report within 30 days. An internal investigation will be conducted, and appropriate remedial actions will be taken in cooperation with the affected districts (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Districts have continuous access to the student data collected through Launchpad and may request reviews, updates, or</p>
---	--	---

		<p>deletions. Skills21 provides direct support for all privacy-related inquiries via email or phone during standard business hours (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii–iii and Section 7.a.i – Additional Provisions and Contact and Support).</p>
2	<p>Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.</p>	<p>Administratively, Skills21 at EdAdvance enforces strict internal policies governing data access, retention, and disclosure. It upholds a clear protocol for responding to requests for access, corrections, or deletions of student data by students, parents, guardians, or school districts. In the event of a data breach, the organization commits to notifying affected districts within 48 hours and delivering a detailed report within 30 days, followed by a full investigation and remediation process in coordination with the affected parties (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i–iii – Additional Provisions).</p> <p>Operationally, Skills21 ensures that all personnel who handle student data are aware of and trained in relevant data privacy and security practices. The organization enables school districts to view and manage all student data submitted through Launchpad and provides responsive support services for privacy-related inquiries during standard hours (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii and Section 7.a.i – Additional Provisions and Contact and Support).</p> <p>Technically, all student data is stored in a secure web-based storage system equipped with layered security features to prevent unauthorized access or use. These features include encryption, secure authentication protocols such as Google Single Sign-On (SSO), and secure infrastructure practices. Skills21's use of artificial intelligence tools, like the ChatGPT API, is also managed under contracts that prevent data retention by third parties and ensure compliance with applicable laws (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data; Section 3.a.iii – Definitions of Student Data).</p>
3	<p>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.</p>	<p>Personnel involved in the handling of student data are expected to operate under the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Connecticut Student Data Privacy Act. Skills21 at EdAdvance affirms its compliance with these laws and maintains policies and procedures intended to safeguard the confidentiality, integrity, and security of student data (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii and Section 5.a.iv – Governing Laws; Retention of Student Data).</p>

4	<p>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.</p>	<p>All parties involved in handling student data are expected to adhere to the applicable legal and contractual standards (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws). employees and subcontractors engaged in the provision of services are subject to internal policies and confidentiality requirements that reflect these obligations. Skills21’s operational emphasis on secure data handling, limited use of third-party tools, and coordinated incident response support an overarching governance model that ensures alignment with applicable data privacy laws and contractual requirements (Skills21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv and 6.a.i – Retention of Student Data; Additional Provisions).</p>
5	<p>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.</p>	<p>In the event of a data security or privacy incident involving personally identifiable information (PII), Skills21 at EdAdvance has established response protocols designed to ensure timely containment, investigation, and notification in accordance with applicable legal obligations.</p> <p>Upon discovery of a breach affecting student data, Skills21 will notify the Educational Authority (EA) and all affected school districts via email within 48 hours. A comprehensive breach report identifying the students involved and the nature of the compromised information will be provided within 30 days. Following notification, Skills21 will either (A) conduct an investigation to determine the scope and impact of the unauthorized disclosure or (B) restore the reasonable integrity of the compromised system. In either case, Skills21 will cooperate fully with affected districts to fulfill legal obligations related to notification, investigation, remediation, and compliance (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Although the organization’s detection practices are not described in detail, Skills21 affirms that all student data is stored in secure, web-based systems protected by layered security measures, and that such safeguards are intended to prevent unauthorized access or breaches (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data). The organization also provides support channels to facilitate timely communication and corrective action.</p> <p>This framework ensures that Skills21's incident response aligns with federal and state data privacy laws and maintains</p>

		transparency and accountability in managing incidents that implicate PII.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	<p>When data maintained by Skills21 is no longer needed to fulfill contractual obligations, or upon termination of the agreement, the organization adheres to a defined data retention and deletion protocol as outlined in its privacy policy.</p> <p>Upon conclusion of services, student data will be deleted unless a specific retention provision has been agreed to, or unless the data is otherwise subject to legal preservation requirements. School districts, including the Educational Authority, may issue a written request identifying the data to be deleted. Skills21 will comply with such requests, provided the data is not required to be retained under state or federal law or stored solely within inaccessible disaster recovery systems (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.i-ii – Retention of Student Data).</p> <p>Skills21 affirms that all content created by students remains the property of the student and their parent or guardian, and that EdAdvance does not own or claim control over student data. Therefore, the district retains full authority to direct data disposition, including deletion or any applicable transfer, when the contract ends (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iii – Retention of Student Data).</p>
7	Describe your secure destruction practices and how certification will be provided to the EA.	<p>When data is no longer needed to meet contractual obligations, or upon request by a school district such as the Educational Authority (EA), Skills21 will delete the specified student data unless retention is required by law or it exists solely within an inaccessible disaster recovery system. Deletion will be executed through industry-standard secure methods that prevent recovery or unauthorized access (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.ii and 5.a.iv – Retention of Student Data).</p>
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	<p>Skills21 explicitly complies with both the Family Educational Rights and Privacy Act (FERPA) and the Connecticut Student Data Privacy Act (CGS §10-234aa to 10-234ff). These laws are commonly embedded in EA data governance frameworks and dictate the lawful handling of student personally identifiable information (PII) (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws).</p> <p>Skills21 recognizes that student data is not the property of EdAdvance, and ownership remains with the student and the educational entity. This is consistent with EA policies that</p>

		<p>prioritize local control and transparency over student information. Districts have continuous access to a registry of data collected from their students and may request corrections or deletions at any time (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iii and Section 6.a.ii – Retention of Student Data; Additional Provisions).</p> <p>Data is stored in secure web-based systems protected against unauthorized access. In the event of a breach, Skills21 commits to:</p> <p>Notifying the EA within 48 hours,</p> <p>Providing a breach report within 30 days, and</p> <p>Cooperating fully in the investigation and remediation process (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Skills21 supports the right of parents, students, and districts to review and correct PII, which is central to FERPA and mirrored in most EA privacy policies. Requests must follow district procedures, and EdAdvance will assist as necessary (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.iii – Additional Provisions).</p>
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	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	Skills21 clearly defines the types of Student Data collected and used, including names, email addresses, gender, school, grade,

Function	Category	Contractor Response
	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.	<p>and race, along with the purpose of use, such as student account creation, analytics, and grant reporting (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 3.a.i-iv and Section 4.a.i-iii – Definitions and Use of Student Data).</p> <p>The organization uses Google Single Sign-On (SSO) for account creation, which ensures secure authentication and user-specific access control. Student data is hosted in secure web-based storage systems, designed with protective measures against unauthorized access (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>Skills21 manages personnel access to student data according to role and necessity, and restricts data use to educational and administrative purposes only. Districts retain ownership and control, further supporting a governance model that respects data sensitivity and organizational priorities (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iii – Retention of Student Data).</p>
	<p>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.</p>	<p>Skills21 at EdAdvance's mission is to provide "flexible, affordable, and road-tested models for driving student success" using digital learning platforms. The Launchpad system supports challenge-based learning and student innovation, which defines the core educational objectives that drive data handling and system usage (Skills21 Launchpad Terms of Service – Introduction; Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 2.a.i – Details of the Policy).</p> <p>Stakeholders include students, parents or guardians, school districts, teachers, and program administrators. Skills21 recognizes the legal and ethical rights of these stakeholders, particularly around ownership, access, and correction of student data. This stakeholder-centered approach informs privacy-related responsibilities and aligns with EA and regulatory expectations (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Sections 4, 5, and 6 – Use and Retention of Student Data, Additional Provisions).</p> <p>Skills21 assumes specific privacy-related responsibilities such as:</p> <ul style="list-style-type: none"> Ensuring secure data storage, Responding to data breach incidents, Assisting districts with access, correction, or deletion requests <p>(Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i-iii – Additional Provisions; Section 7.a.i – Contact and Support).</p> <p>Skills21 Launchpad's data handling practices are structured to comply with FERPA and Connecticut's Student Data Privacy Act. These statutes inherently incorporate risk management requirements concerning the protection of personally identifiable information (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws).</p>
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational</p>	<p>Skills21 explicitly affirms its compliance with both the Family Educational Rights and Privacy Act (FERPA) and the Connecticut Student Data Privacy Act (CGS §10-234aa–10-234ff). These laws are directly incorporated by reference into the privacy policy. This</p>

Function	Category	Contractor Response
	requirements are understood and inform the management of cybersecurity risk.	<p>ensures that the organization's data practices are governed by statutory protections for personally identifiable information (PII) (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws).</p> <p>Skills21 maintains a defined privacy policy that governs the collection, use, storage, and deletion of student data. Key provisions include:</p> <p>Permitted uses of student data (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 4.a.i-iii),</p> <p>Student data retention and deletion rights (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.i-ii),</p> <p>Data breach response and district notification protocols (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i),</p> <p>District oversight of student data accuracy and access (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii-iii).</p> <p>These provisions provide a formal structure for managing privacy and cybersecurity risks within educational operations.</p> <p>The organization's breach response process includes notifying affected school districts within 48 hours of a data breach and providing a comprehensive report within 30 days, followed by remediation and cooperation in legal compliance efforts (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Skills21 provides access to data records for each school district and supports correction and deletion requests. It offers dedicated support contact information and procedures to address inquiries related to student data (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 7.a.i – Contact and Support).</p>
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>Skills21 at EdAdvance identifies the handling of student personally identifiable information (PII) as a critical operational risk. The organization's data privacy policy acknowledges that misuse, unauthorized access, or breaches could affect students' rights, district obligations, and the organization's legal standing. This recognition extends to the use of secure platforms and tools (e.g., Google Single Sign-On), and to the storage of data in protected web-based systems (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 3.a-5.a – Definitions, Use, and Retention of Student Data).</p> <p>Skills21 adheres to FERPA and Connecticut's Student Data Privacy Act, which reduces legal liability and protects the integrity and mission of Skills21's educational programs. By committing to legal compliance and transparent data practices, the organization safeguards its image and functional continuity (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws).</p> <p>Skills21's breach notification procedures reflect a recognition of the operational and reputational harm that may result from</p>

Function	Category	Contractor Response
		<p>unauthorized disclosures. (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Skills21 understands that failure to manage privacy risks can impact not only the organization but also individuals and educational authorities. For example, students and guardians are granted rights to request corrections or deletions of erroneous data, and school districts are given full access to student data records and deletion mechanisms (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii-iii – Additional Provisions).</p>
	<p>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>Skills21 prioritizes compliance with FERPA and the Connecticut Student Data Privacy Act, establishing these as the primary legal constraints and operational guardrails for managing student data. The organization’s central objective: to support educational innovation and student engagement through its Launchpad platform, guides its decisions on what data to collect, how to use it, and the safeguards to implement (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii – Governing Laws; Section 4.a.i-iii – Use of Student Data).</p> <p>Skills21 demonstrates a low risk tolerance with respect to unauthorized access, breaches, or misuse of student PII. This is evident in its use of secure authentication (Google SSO), commitment to secure web-based storage, and clear boundaries around data usage (e.g., analytics, account creation, and de-identified grant reporting only) (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>The organization's prohibition against unauthorized data retention or access, to include use of third-party technologies like the ChatGPT API, further illustrates conservative assumptions about data exposure risks (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv).</p> <p>In the event of a breach, Skills21 has codified response procedures that reflect both legal compliance and risk-mitigating priorities. These include 48-hour breach notification, 30-day detailed reporting, and full cooperation with school districts to remediate harm (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions). This approach aligns with a risk strategy that seeks to minimize impact and maintain institutional trust.</p>
	<p>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.</p>	<p>Skills21 Launchpad utilizes Google Single Sign-On (SSO) for account creation and authentication. The Privacy Statement acknowledges the use of OpenAI’s ChatGPT API as part of system functionality. In both cases, Skills21 affirms that these third-party tools are governed by contracts and practices consistent with Connecticut’s Student Data Privacy Act, and that no student data is added to external training datasets or misused by vendors (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 3.a.iii; Section 5.a.iv – Definitions and Retention of Student Data).</p> <p>Skills21 emphasizes that all technologies used are contractually bound to comply with student data privacy laws.</p>
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to	Skills21 Launchpad uses Google Single Sign-On (SSO) for account creation and login. This method supports secure, role-based

Function	Category	Contractor Response
	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.	<p>authentication and limits access to authorized users by leveraging trusted identity verification from Google accounts. Through this system, only users with valid credentials (students, educators, or district personnel) are granted access to Launchpad services (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 3.a.iii – Definitions of Student Data).</p> <p>Student data is hosted in secure web-based storage systems, and access is limited to authorized personnel for educational and administrative purposes only. Skills21 explicitly states that it takes “all necessary action to ensure the confidentiality and security of Student Data,” including the implementation of security measures to prevent unauthorized access (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>Districts maintain ownership and oversight of student data. They have the right to review, correct, or request deletion of data at any time, reinforcing localized control over access and data accuracy (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii – Additional Provisions). Furthermore, requests for access or updates by students or guardians must be submitted through the school district, in alignment with FERPA regulations, ensuring data access is mediated and verified through authorized institutional channels (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.iii).</p>
	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.	Skills21 ensure that relevant staff are aware of their obligations to protect data confidentiality and respond appropriately to privacy incidents (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Sections 5.a.iv and 6.a.i – Retention of Student Data; Additional Provisions).

Function	Category	Contractor Response
	<p>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.</p>	<p>Skills21 ensures the confidentiality of student data through the use of secure web-based storage systems with multiple protective layers designed to prevent unauthorized access. All data collected, such as student names, emails, school information, and demographic details, is managed in compliance with FERPA and the Connecticut Student Data Privacy Act, and cannot be disclosed or accessed beyond authorized educational purposes (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>Districts retain ownership and control of all student data. They may access, correct, or request the deletion of such data at any time. Skills21 will also support districts and guardians in ensuring data accuracy, thereby preserving the integrity of records over time (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii-iii – Additional Provisions). Data may also be used for system analytics or aggregated grant reporting, but only in de-identified forms.</p> <p>Skills21 commits to maintaining the availability of student data for educational use until it is no longer needed or a deletion request is received. Special exceptions apply for data retained under legal requirements or disaster recovery systems, which remain inaccessible to the public and unavailable for regular business use (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.i-ii – Retention of Student Data).</p> <p>In the event of a security breach, Skills21 has a defined incident response plan, which includes district notification within 48 hours, detailed breach reporting within 30 days, and subsequent actions to restore the integrity of the data systems (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions). This ensures continued availability and reliability of the platform.</p>
	<p>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.</p>	<p>Skills21 has a clearly articulated privacy policy that outlines the collection, use, storage, and retention of student data in support of its educational platform. This policy incorporates legal requirements under FERPA and the Connecticut Student Data Privacy Act, defining the permissible scope of data use (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 1.a.ii and Section 4.a – Governing Laws and Use of Student Data).</p> <p>Skills21 has codified processes for:</p> <ul style="list-style-type: none"> Data collection via Google SSO, Secure data storage in protected systems, Aggregated data use for grant reporting and analytics, Responding to data deletion or correction requests from districts or guardians, and Incident management, including breach notification and remediation (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Sections 3.a-6.a). <p>These operational procedures demonstrate a structured approach to information protection.</p>

Function	Category	Contractor Response
		Skills21 supports school districts, students, and families in managing student data through dedicated contact channels for inquiries, deletions, or corrections. This underscores the organization's commitment to supporting privacy rights but does not equate to a documented security management policy (Section 7.a.i – Contact and Support).
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	System maintenance activities are performed with security-conscious handling. The use of secure web-based storage systems and structured breach response processes work to ensure system availability and reliability are operational priorities.
	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.	<p>Skills21 Launchpad hosts student data within secure web-based storage systems, which are protected by multiple security measures intended to prevent unauthorized access. These systems are designed to comply with FERPA and the Connecticut Student Data Privacy Act, forming the legal and operational foundation for technical protection of student data (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p> <p>The use of Google Single Sign-On (SSO) for account creation and login ensures secure authentication and controlled access to the Launchpad platform. This approach limits access to authorized users and integrates with widely adopted authentication infrastructure (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 3.a.iii – Definitions of Student Data).</p> <p>Skills21 acknowledges the use of external technologies, such as the ChatGPT API, and explicitly states that these services are contractually required to adhere to privacy laws. The organization affirms that student data used in conjunction with such tools is protected and not incorporated into external training datasets, thus maintaining the integrity and confidentiality of data during external processing (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv).</p>
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	<p>Skills21 policies demonstrate a clear understanding of the importance of timely breach response and the protection of student data,</p> <p>awareness of incident-related risk. Upon discovery of a data breach, Skills21 is committed to:</p> <p>Notifying affected school districts within 48 hours, and</p> <p>Providing a detailed report within 30 days, including the scope of the incident and identities of affected students (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions). Once an incident is identified, Skills21 procedures assess its impact on individuals and systems, and coordinate remediation (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 5.a.iv – Retention of Student Data).</p>
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<p>Security and system integrity are valued operational priorities (Section 5.a.iv – Retention of Student Data).</p> <p>Skills21's breach response framework, requiring notification within 48 hours and investigation or remediation thereafter, ensure that incidents are taken seriously once identified (Skills 21</p>

Function	Category	Contractor Response
		at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Skills21 is committed to protecting student data in accordance with the Family Educational Rights and Privacy Act (FERPA) and the Connecticut Student Data Privacy Act. Skills21 maintains security practices and system configurations designed to identify unauthorized access and other irregularities that may compromise data integrity (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Sections 5.a.iv and 6.a.i – Retention of Student Data; Additional Provisions).
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	<p>In the event of a data security breach involving student data, Skills21 is contractually committed to:</p> <p>Notifying affected school districts within 48 hours of discovering the breach, and</p> <p>Providing a detailed report within 30 days, including the names of affected students and the nature of the compromised data.</p> <p>Following the breach, Skills21 will either:</p> <p>Conduct an investigation to assess the scope and impact of the incident, or</p> <p>Restore the reasonable integrity of the data system.</p> <p>These actions will be carried out in coordination with the affected districts, ensuring legal compliance and facilitating remediation (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p>
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	<p>In the event of a breach involving personally identifiable student data, Skills21 commits to:</p> <p>Notifying affected school districts within 48 hours of discovery,</p> <p>Providing a detailed breach report within 30 days, which includes the identity of affected students and the nature of the data compromised,</p> <p>Cooperating fully with the affected school districts in fulfilling their legal obligations, including investigation, remediation, and notification of individuals, as required by law (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>Skills21 will support school districts in meeting their legal obligations related to breach notification and data correction. Skills21 also facilitates data access and correction requests by routing such communications through district procedures, ensuring all actions are consistent with district policies and FERPA regulations (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.ii–iii).</p>
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	<p>In the event of a cybersecurity incident involving student data, Skills21 commits to:</p> <p>Conducting an investigation to determine the nature and scope of the unauthorized access, disclosure, or acquisition,</p>

Function	Category	Contractor Response
		<p>Identifying the students whose information was compromised, and</p> <p>Supporting the affected districts in their efforts to understand and remediate the breach (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>This analysis is part of a broader breach response process designed to facilitate recovery and fulfill legal obligations. It reflects an acknowledgment of the need to assess impact and determine root causes.</p> <p>Skills21’s involvement includes working with districts to restore the integrity of data systems, which implies the use of analytical findings to inform technical remediation and risk reduction. The cooperation clause further reinforces that analysis is not siloed but integrated with the broader recovery and compliance process.</p>
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>Following the discovery of a data breach, Skills21 is contractually obligated to:</p> <p>Notify affected school districts within 48 hours,</p> <p>Provide a detailed report within 30 days, and</p> <p>Either conduct an investigation to assess the scope and cause of the incident or restore the reasonable integrity of the affected data systems (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p> <p>These steps are aimed at preventing the expansion of the breach and resolving the underlying vulnerability that led to unauthorized access or disclosure.</p> <p>Collaboration with Affected Entities Skills21 commits to cooperating with school districts in executing all required legal and technical remediation activities, including notification of affected individuals and system restoration. This reinforces a mitigation approach that prioritizes coordinated response, limits further exposure, and supports affected stakeholders in managing the aftermath.</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>Skills21 is committed to maintaining data protection practices that align with FERPA and the Connecticut Student Data Privacy Act. Skills21 maintains an operational readiness to assess and address cybersecurity incidents through structured investigation, system restoration, and full cooperation with school districts. These response activities, coupled with the organization's commitment to safeguarding student data, ensure that lessons are learned from incidents and evaluated to inform future procedural adjustments (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad –Section 6.a.i – Additional Provisions).</p>
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>In response to a breach or unauthorized data disclosure, Skills21 is obligated to:</p> <p>Conduct an investigation to determine the nature and scope of the incident, or</p> <p>Restore the reasonable integrity of the data system that was compromised (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p>

Function	Category	Contractor Response
		Skills21 agrees to cooperate with school districts to carry out their legal obligations, which may include recovery activities such as restoring data, remediating system vulnerabilities, and supporting communications with affected individuals.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Skills21 is committed to ensuring the integrity and availability of student data in accordance with FERPA and the Connecticut Student Data Privacy Act. Skills21's incident response process includes investigative steps and coordinated remediation with school districts. This cooperative framework supports reflective evaluation of incidents and the adaptation of recovery practices based on prior experience (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad –Section 6.a.i – Additional Provisions). Through its privacy-focused operational model and district engagement, Skills21 continuously seeks to refine its recovery processes in support of secure, resilient service delivery.
	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).	<p>In the event of a breach, Skills21 is required to:</p> <p>Notify affected school districts within 48 hours, and</p> <p>Provide a detailed breach report within 30 days, including the scope of the incident and affected student data.</p> <p>Skills 21 commits to cooperating fully with school districts to carry out necessary remediation, restoration of system integrity, and legal compliance measures (Skills 21 at EdAdvance Privacy Policy for Skills21 Launchpad – Section 6.a.i – Additional Provisions).</p>