Cornwall Central School District

and

Snorkl Inc.

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

ARTICLE: 1 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 01/14/2026 ("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**.

Contactor 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: Megan Argenio

Title: Superintendent of Schools

Address: 24 Idlewild Avenue

City, State, Zip: Cornwall-On-Hudson, NY 12520

Email: margenio@cornwallschools.com

Name: Karen Brooks

Title: Director of Data and Instructional Technology

Address: 24 Idlewild Avenue

City, State, Zip: Cornwall-On-Hudson, NY 12520

Email: kbrooks@cornwallschools.com

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: *[Signature]* Karen Brooks	BY: *[Signature]* Jeffrey Plourd
[Printed Name] Karen Brooks	*[Printed Name]* Jeffrey Plourd
[Title] Director of Data & Instructional Tech	[Title] CEO
Date: 1/13/26	Date: 1/14/2026

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: kbrooks@cornwallschools.com. (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.

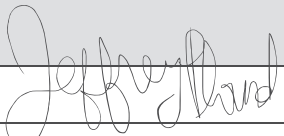
CONTRACTOR	
[Signature]	
[Printed Name]	Jeffrey Plourd
[Title]	CEO
Date:	1/14/2026

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). Contractor to complete.

Name of Contractor	Snorkl, Inc
Description of the purpose(s) for which Contractor will receive/access PII	Snorkl uses personally identifiable information (PII) collected through its platform solely to provide and improve the educational services we offer to schools and districts. The specific purposes for which PII is used include: 1. Account Management: PII is used to create and manage user accounts on the Snorkl platform. This includes maintaining user
Type of PII that Contractor will receive/access	Check all that apply: ■ Student PII ☐ APPR Data
Contract Term	Contract Start Date January 2026 Contract End Date January 2029
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) ☐ Contractor will not utilize subcontractors. ■ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • 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	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: 1. Secure Data Centers: PII is stored in secure data centers managed by reputable third-party service providers, including Amazon Web Services (AWS) and Render. These data centers are located in the United States and are equipped with state-of-the-art physical and environmental controls to safeguard the data against unauthorized access, natural disasters, and other potential threats. 2. Data Encryption: All PII stored within our data centers is encrypted both at rest and in transit using advanced encryption standards (AES-256). This ensures that even if data is intercepted during transmission, it remains unreadable without the correct decryption keys. 3. Access Controls: Access to PII stored in our data centers is strictly controlled through the use of role-based access controls (RBAC), which ensure that only authorized personnel have access to sensitive data. These controls are enforced through unique user credentials and multi-factor authentication. 4. Regular Audits and Compliance: Our data storage facilities undergo regular security audits and compliance checks to
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Jeffrey Plourd
[Title]	CEO -
Date:	1/14/2026

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.**

Please see the table below

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	
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.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
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 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.	
	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.	
	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.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	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	

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
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.	
	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.	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	Information 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.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	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.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	

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.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
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.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	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).	

EXHIBIT C - Contractor's Data Privacy and Security Plan

I. Outline how you will implement applicable data security and privacy contract requirements over the life of the contract.

Snorkl implements robust security and privacy protections aligned with both federal and state laws. Over the life of the contract, we will:

- **Ensure compliance with all regulatory frameworks** including COPPA, FERPA, and applicable state privacy laws, ensuring that PII (Personally Identifiable Information) is handled according to these requirements.
- **Incorporate contractual terms** for data security and privacy in agreements with all subprocessors, ensuring they adhere to the same standards.
- **Maintain a data processing agreement (DPA)** with clear provisions that define Snorkl's role as a data processor, and specify responsibilities for both the controller (the organization) and Snorkl.
- **Regularly audit subprocessors** such as AWS, Render, and OpenAI, ensuring they remain SOC 2 compliant and maintain the same level of data protection.
- **Regularly review internal policies** to ensure evolving regulatory requirements are incorporated and that Snorkl maintains up-to-date compliance.

II. Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.

Snorkl employs a combination of administrative, operational, and technical safeguards to protect PII, including:

- **Administrative Safeguards**:
  - **Data Classification and Access Control**: PII is tagged and classified based on sensitivity, with access restricted using role-based access control (RBAC). Only authorized personnel can access sensitive data.
  - **Vendor Management**: Subprocessors are bound by stringent contractual obligations, ensuring they comply with all privacy requirements.
  - **Incident Response Plan**: Regularly tested incident response plans ensure Snorkl responds to security incidents promptly and effectively.
- **Operational Safeguards**:
  - **Data Processing Agreement**: Outlines the specific data processing terms between Snorkl and organizations, ensuring compliance with all privacy regulations.
  - **Training Programs**: Mandatory privacy and security training via Huntress MyCurricula ensures employees and contractors are educated on federal and state privacy laws.
  - **Data Retention Policy**: Ensures PII is only retained for as long as necessary and is securely deleted afterward.

- **Technical Safeguards**:
    - **Encryption**: PII is encrypted both at rest (using AES-256 encryption) and in transit (via TLS 1.2).
    - **Continuous Monitoring**: Systems are monitored using AWS CloudTrail and CloudWatch to detect anomalies, and tools like LogRocket are used to monitor user behavior.
    - **Secure Authentication**: All access to PII is protected by multi-factor authentication and secure password management systems.

III. 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.

Snorkl employees and subcontractors undergo mandatory cybersecurity and privacy training via **Huntress MyCurricula.** This training covers:

- **Federal laws**: Including COPPA, FERPA, and other relevant laws that govern the confidentiality of PII in educational settings.
- **State-specific regulations**: Such as the California Consumer Privacy Act (CCPA) and similar privacy laws across other states (Nevada, Colorado, Utah, etc.).
- **Data protection practices**: Training also includes guidelines on handling PII, secure communication practices, and the legal implications of data breaches.
- **Ongoing training**: Regular updates ensure that employees remain knowledgeable about any changes to privacy laws and new security threats.

IV. 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 employees and subcontractors are required to sign legally binding agreements that:

- **Define data protection requirements**: Employees are contractually bound to protect PII in compliance with all applicable laws.
- **Include confidentiality clauses**: Employees and subcontractors agree to handle PII with the highest confidentiality.
- **Data Processing Agreement for Subprocessors**: Snorkl contracts subprocessors (such as AWS, Render, and OpenAI) under a Data Processing Agreement (DPA) that mirrors the privacy and security obligations in our contracts with clients.
- **Termination clauses**: In case of a breach of privacy obligations, the contract outlines penalties and immediate actions, including termination of the agreement.

V. 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.

Snorkl's incident management plan includes:

- **Incident Response Plan**: An established, tested incident response plan that covers the identification, containment, and resolution of security incidents.
- **Breach Detection**: Continuous monitoring using AWS CloudTrail, CloudWatch, Render Metrics, and LogRocket allow us to detect breaches and unauthorized disclosures in real-time.
- **Notification Procedures**: In the event of a data breach, Snorkl is committed to:
    - Notifying affected entities (including the EA) within 72 hours.
    - Providing a detailed report outlining the nature of the breach, affected individuals, and mitigation steps.
- **Mitigation and Remediation**: We immediately isolate affected systems, contain the breach, and work with the EA to mitigate its impact.
- **Post-Incident Reviews**: All incidents undergo a post-incident analysis to identify root causes and improve future prevention.

VI. Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.

When data is no longer needed to meet contractual obligations, Snorkl will:

- **Coordinate with the EA**: We will work with the EA to define the transfer process, ensuring data is securely transitioned back to the EA or securely destroyed as per EA requirements.
- **Data Transfer**: If applicable, data is securely transferred to the EA using encrypted file transfers, ensuring it remains protected during the handover process.
- **Data Deletion**: Upon confirmation of a successful transfer, Snorkl will securely delete any remaining data in its possession, ensuring compliance with privacy regulations.

VII. Describe your secure destruction practices and how certification will be provided to the EA.

Snorkl adheres to industry-standard practices for the secure destruction of data:

- **Secure Deletion**: We use encryption-based deletion methods for data stored in cloud services (AWS, Render). This includes overwriting data to ensure it cannot be recovered.
- **Certificate of Destruction**: After data is destroyed, Snorkl will provide a certificate of destruction via email to the EA, outlining:
    - The type of data destroyed.

    - The method used for destruction.
    - The date of destruction.

VIII. Outline how your data security and privacy program/practices align with the EA's applicable policies.

SnorkI's data security and privacy practices align closely with the EA's privacy policies as follows:

- **Compliance with Privacy Policies**: SnorkI only processes PII in accordance with the EA's privacy requirements and ensures that all subprocessors are contractually bound to adhere to the same standards.
- **Data Minimization**: SnorkI collects only the minimum required PII necessary for the operation of its platform, ensuring compliance with data minimization principles.
- **Third-Party Management**: Subprocessors (AWS, Render, OpenAI, etc.) are required to maintain SOC 2 compliance and are regularly audited to ensure they align with the EA's privacy standards.

Exhibit C.1 – NIST CSF Table

NIST Cybersecurity Control Framework (CSF) Version 1.1

Domain	NIST Category	Framework Objective	Snorkl, Inc. Implementation
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.	Snorkl maintains a comprehensive asset inventory system where data, personnel, devices, and systems are tagged and classified based on their sensitivity and importance. This tagging system ensures that critical assets like PII (personally identifiable information) are managed appropriately. Render and AWS are key subprocessors managing Snorkl's databases, and their compliance programs support the use and ability to securely store data.
	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.	Snorkl's mission to provide an AI-driven feedback platform is central to its cybersecurity program. The organization prioritizes protecting student and educational data. Cybersecurity is an important business function that is supported at the company's senior levels. Snorkl engages with security and data privacy experts to ensure that Snorkl maintains cyber resilience, ensures business continuity, and is focused on current, and emerging risks that may affect the organization, our people, our assets, and our customers.
	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.	Snorkl's governance policies ensure that data is handled in compliance with regulatory frameworks such as CCPA, COPPA and FERPA., and Contractual Requirements. These policies dictate data classification, risk management, and incident response.
	Risk Assessment (ID.RA):	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Snorkl conducts annual risk assessments, involving management meetings that evaluate the security posture of the platform. The risk assessment process evaluates both the potential impacts and likelihood of risks, ensuring proactive mitigation where necessary. Subprocessors

			such as AWS and OpenAI undergo regular security reviews to ensure they meet Snorkl's security requirements and maintain their SOC 2 certification.
	Risk Management Strategy (ID.RM)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Snorkl's risk management strategy is based on its operational priorities and risk tolerance. Decisions are made using four approaches: acceptance, mitigation, transference, or avoidance. Risk mitigation is prioritized for sensitive data due to the platform's user base, particularly involving minors. AWS and Render, through their secure, SOC 2-compliant environments, play a critical role in supporting Snorkl's risk mitigation strategy.
	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.	Snorkl ensures that all subprocessors, such as AWS, Render, and OpenAI, undergo regular security assessments to meet the organization's security standards. SOC 2 compliance is a key factor in selecting and managing subprocessors. The supply chain risk management process includes verifying the ongoing compliance of subprocessors with applicable security requirements.
Protect (PR)	**Identity Management, Authentication and Access Control (PR.AC)**	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.	Snorkl employs role-based access control (RBAC) to manage access to its platform, ensuring that access to data is limited to authorized personnel. AWS Identity and Access Management (IAM) and Render's access control systems help manage access to cloud resources, consistent with internal standards. Regular reviews of user roles ensure alignment with the principle of least privilege.
	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.	Snorkl provides comprehensive cybersecurity training via Huntress MyCurricula. All employees and contractors must complete this training during onboarding, and it is regularly updated to reflect new cybersecurity risks. Training focuses on compliance with Security Awareness and Privacy regulations, regarding data security.
	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.	Snorkl implements stringent data security controls, including the encryption of data at rest using AES-256 and in transit via TLS 1.2. AWS provides the underlying cloud infrastructure for secure data storage, while Render and OpenAI adhere to stringent data security practices. Regular audits ensure continued SOC 2 compliance for all subprocessors.
	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	Snorkl has established and documented security policies that are regularly updated to reflect new regulations and standards. Subprocessors like AWS and Render, with their SOC 2 certifications, play an essential role in supporting these information protection processes.

		systems and assets.	
	Maintenance (PR.MA)	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance of Snorkl's information systems, including cloud resources managed by AWS and Render, follows documented procedures to ensure system integrity. Internal policies, ensuring minimal risk to the confidentiality, integrity, and availability of data. Routine system updates and patches are carried out with minimal disruption to users. Vulnerability detection and patching on endpoints is performed on a regular basis. Beyond OS updates, vulnerability scanning includes identification of missing patches in third-party software and detection for potential configuration issues. Identified vulnerabilities are reviewed regularly and communicated to risk owners to promote timely remediation.
	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.	Snorkl employs technical security solutions such as encryption, secure backups, and continuous monitoring to ensure the resilience of its systems and data. Systems networks are protected with next-generation firewalls, integrated with security layers such as Traffic decryption, VPN, URL Filtering, Advanced Threat Analysis, SIEM, DLP and other security tools. Remote access is protected with advanced 2FA, Single Sign On and user VPN in an integrated security approach. AWS and Render provide the infrastructure that enables these solutions, with regular audits and reviews ensuring compliance with SOC 2 security controls. These protective technologies are crucial for maintaining the confidentiality and integrity of user data.
Detect (DE)	**Anomalies and Events (DE.AE)**	Anomalous activity is detected and the potential impact of events is understood	Snorkl uses continuous monitoring tools to detect anomalous behavior within its platform. AWS's CloudTrail and CloudWatch, and Render Metrics to monitor activity on cloud resources, and LogRocket is used to detect unusual user behavior. Regular reviews of logs ensure that any potential security events are quickly identified and mitigated, reducing the risk of data breaches. AWS and Render's SOC 2 compliance ensures the integrity of cloud infrastructure.
	Security Continuous Monitoring (DE.CM):	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Snorkl implements continuous monitoring of all systems and assets using AWS CloudTrail, CloudWatch, Render Metrics, and LogRocket to monitor user interactions and detect suspicious behavior. AWS provides real-time visibility into cloud activities, ensuring that any anomalies are immediately addressed. Regular reviews of these systems are conducted to ensure the

			effectiveness of Snorkl's protective measures, and subprocessors are required to maintain SOC 2 compliance.
	Detection Processes (DE.DP)	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Snorkl has formalized and documented detection processes that are tested regularly to ensure effectiveness. The detection mechanisms include automated alerts for unusual activity and are integrated with AWS's cloud monitoring services. These processes are aligned with SOC 2 standards, and subprocessors like Render also participate in testing detection processes to ensure full integration across the supply chain.
Respond (RS)	**Response Planning (RS.RP)**	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Snorkl has established incident response plans that are regularly tested and updated. These plans include clear roles and responsibilities for all involved parties, including subprocessors like AWS and Render. Regular tabletop exercises and incident response drills are conducted to ensure all personnel are prepared to handle cybersecurity incidents efficiently. The SOC 2-compliant subprocessors adhere to these plans to ensure coordinated responses to security incidents.
	Communications (RS.CO)	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Snorkl maintains a clear communication plan for coordinating with both internal and external stakeholders during a security incident. This includes notifications to schools and educational institutions, as well as relevant subprocessors like AWS, Render, and OpenAI. External agencies such as law enforcement are engaged when necessary. All subprocessors follow communication protocols, ensuring transparency and efficient coordination.
	Analysis (RS.AN)	Analysis is conducted to ensure effective response and support recovery activities.	After any incident, Snorkl conducts a post-incident analysis to identify root causes and improve future responses. Subprocessors such as AWS and Render provide detailed incident reports as part of their SOC 2 compliance, ensuring that lessons learned are fully integrated into future operations. These analyses help improve Snorkl's incident response capabilities and reduce the risk of recurrence.
	Mitigation (RS.MI)	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Snorkl's incident response plan includes clear steps for mitigating the impact of security events. This includes isolating affected systems and working with AWS and Render to ensure rapid resolution of the issue. Currently, we have adapted agile compliance measures to ensure that mitigation actions are effectively implemented, and all subprocessors are included in the incident resolution process to prevent the spread of the issue.

	Improvements (RS.IM):	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Lessons learned from previous incidents are used to continuously improve Snorkl's response activities. Incident debriefs are conducted with all subprocessors, including AWS and Render, to integrate improvements into the system. These updates ensure that Snorkl's incident response process remains aligned with evolving cybersecurity risks and industry best practices, maintaining compliance for all subprocessors.
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.	Snorkl has detailed recovery procedures in place, which include backups stored on SOC 2-compliant infrastructure provided by AWS. Regular testing of recovery procedures ensures that systems and data can be restored quickly and efficiently after an incident. Render and other subprocessors participate in recovery planning exercises to ensure that all systems are returned to normal operations as quickly as possible, with minimal impact on users.
	Improvements (RC.IM)	Recovery planning and processes are improved by incorporating lessons learned into future activities.	Snorkl regularly reviews and updates its recovery procedures based on lessons learned from past incidents. Subprocessors like AWS and Render contribute to this process, ensuring that recovery plans are continuously improved to align with best practices. Recovery procedures are documented and tested frequently to ensure readiness for 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).	Snorkl ensures that restoration activities are coordinated with all relevant internal and external parties. This includes schools, educational institutions, subprocessors like AWS, Render, and other vendors. Regular updates are provided throughout the recovery process, ensuring transparency and efficient coordination. All subprocessors adhere to approved communication protocols during recovery operations to ensure timely restoration of services.