

TEMPLATE AGREEMENT¹**EAST RAMAPO CENTRAL SCHOOL DISTRICT
DATA PRIVACY AGREEMENT****EAST RAMAPO CENTRAL SCHOOL DISTRICT
and**

This Data Privacy Agreement ("DPA") is by and between the East Ramapo Central School District, ("EA"), an Educational Agency, and Capstone ("Contractor"), collectively, the "Parties". This DPA is a rider to the Service Agreement dated July 1, 2022 that governs the provision of PebbleGo/PebbleGo Next to the EA.

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.

¹This is a template agreement only, and its terms and conditions may be subject to change.

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 student 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 student 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 July 1, 2022 (the "Service Agreement"); Contractor may receive PII regulated by applicable 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 unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

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

8. Termination

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

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA. 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 as prescribed in this Agreement. 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) 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) Upon request, 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) calendar 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 mail, 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: Bhavin Gandhi
Title: Data Protection Officer
Address: 105 S. Madison Avenue
City, State, Zip: Spring Valley, NY 10977
Email: DPO@ercsd.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 of data governed by this Agreement. 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.


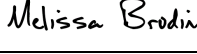
EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY: 
Bhavin Gandhi	Melissa Brodin <small>7F5901D797804C5...</small>
Director of Information Technology	Director Contracts, Compliance, and Data Privacy
Date: 7-7-2021	Date: 08/02/2022

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

The East Ramapo Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information in educational records from unauthorized access or disclosure in accordance with Education Law § 2-d, and all other applicable State and Federal laws.

The East Ramapo Central School District establishes the following Parents' Bill of Rights in which parents, legal guardians, persons in parental relationships, and/or Eligible Students, 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 to: Bhavin Gandhi, Data Protection Officer at DPO@ercsd.org or 845-577-6081; (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.

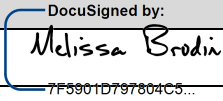
CONTRACTOR	
Signature	Capstone 
Printed Name	Melissa Brodin <small>7F5901D797804C5...</small>
Title	Director Contracts, Compliance, and Data Privacy
Date:	08/02/2022

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	Capstone- PebbleGo/PebbleGo Next
Description of the purpose(s) for which Contractor will receive/access PII	<p>Capstone Digital Products such as PebbleGo (including PebbleGo Next), Capstone Connect, and Capstone Interactive do not have individual student accounts, but rather a single building account shared by all students and educators. PebbleGo, Capstone Connect, and Capstone Interactive do not collect PII, including Student PII.</p> <p>Capstone Digital Products such as PebbleGo Create (an add-on to PebbleGo) and Buncee are creation tools that allow students, educators, and administrators to create and publish original and authentic content. These products do have individual student accounts which can be created by syncing Google Classroom roster data or Microsoft 365 roster data with PebbleGo Create, or manual upload via CSV. With PebbleGo Create and Buncee, students are not required to submit email, gender, or DOB. Capstone does not collect, sell, rent, or otherwise provide personally identifiable information ("PII") to any third parties for advertising or marketing purposes. The purpose(s) for which Contractor will receive/access PII under the PebbleGo Create and Buncee products is outlined below:</p> <p>The purpose of data processing for the PebbleGo Create and Buncee products is to allow Contractor to provide the requested Services to the Educational Agency ("EA") and perform the obligations under the Contract. More specifically, the purpose of processing data is to enable school oversight and ensure appropriate structure and interaction within a school account using PebbleGo Create and/or Buncee. The processing of data enables the interaction, communication, creation and sharing within the classroom/school/district account; allows educators and/or administrators to monitor accounts, set permissions and deliver educational content; allows educators to differentiate and personalize a student's educational experience; and provides the admin-educator-student hierarchy within the account. Contractor requires data capture and use for the following reasons:</p> <ul style="list-style-type: none"> • To confirm the identity of students and educators/administrators • To provide educational services and content • To allow subscribers to create and manage classes, personalize and
	<p>differentiate instruction, and monitor and assess student progress</p> <ul style="list-style-type: none"> • To allow subscribers to monitor and safeguard student welfare

	<ul style="list-style-type: none"> To allow subscribers to set creation and sharing permissions and privacies schoolwide To inform existing subscribers about feature updates, site maintenance, and programs/initiatives (does not include student subaccounts)
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR Data</p>
Contract Term	<p>Contract Start Date July 1, 2022</p> <p>Contract End Date June 30, 2023</p>
Subcontractor Written Agreement Requirement	<p>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)</p> <p><input type="checkbox"/> Contractor will not utilize subcontractors.</p> <p><input checked="" type="checkbox"/> Contractor will utilize subcontractors.</p>
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

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:

Data Storage, Retention, and Access:

User data is stored in secure and managed cloud repositories, accessible only to select development team members via secure connections. Background checks are performed on all employees. Data is backed up routinely, and securely in our cloud infrastructure. Stale data copies are permanently purged. All system identifiers for *user*, *Buncee*, *class* and other entities are randomly generated hexadecimal strings and stored as binary strings. Furthermore, sensitive data like passwords created or changed after 02/2017 are encrypted using modern encryption techniques.

All user data, including file uploads are stored in our secure cloud VPCs.

The Buncee application does not store any user data outside of the United States. However, the Buncee application utilizes Amazon's content delivery network, *CloudFront* to securely deliver rich media to its viewers across the world, which might be temporarily cached by the edge servers.

Measures to Protect Data:

Capstone Digital Products use HTTPS connections to secure transmissions. A combination of firewalls, security keys, SSL certificates, and non-default username/password credentials secure data access. Additionally, the Buncee application has the following preemptive safeguards in place to identify potential threats, manage vulnerabilities and prevent intrusion:

- All security patches are applied routinely
- Server access logging is enabled on all servers
- Fail2ban (an intrusion prevention software framework that protects servers from brute-force attacks) is installed on all servers and will automatically respond to illegitimate access attempts without intervention from engineers
- Our database servers are not publicly accessible via the internet.
- SSH key-based authentication is configured on all servers

Capstone Digital Products use HTTPS connections to secure transmissions. The HTTPS you see in the URL of your browser means when you go to the website, you're guaranteed to be getting the genuine website. With HTTPS in place, all interactions with Capstone Digital Products will be undecipherable

	<p>by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic.</p> <p>Capstone Digital Products use SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees in PebbleGo Create and the Buncee products) is encrypted at rest. All passwords are encrypted using modern encryption technologies.</p> <p>Account information is stored in access-controlled VPCs operated by industry leading partners. All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.</p> <p>The Buncee application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption.</p>
Encryption	Data will be encrypted while in motion and at rest.

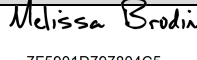
CONTRACTOR	
Signature	<p>DocuSigned by: </p>
Printed Name	<p>7F5004D797004G5... Melissa Brodin</p>
Title	Director Contracts, Compliance, and Data Privacy
Date:	08/02/2022

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.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<p>Throughout the life of the contract, Contractor will:</p> <ul style="list-style-type: none"> • limit internal access to education records to those individuals that are determined to have legitimate educational interests • not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third- Party for marketing or commercial purposes • except for authorized representatives of the Contractor to the extent they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order • maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and
---	--	--

		<p>integrity of personally identifiable information in its custody</p> <ul style="list-style-type: none"> • use encryption technology to protect data while in motion or in its custody from authorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(h)(2) of Public Law §111-5 • adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework • impose all the terms stated above in writing where the Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>Only those who need it to perform their duties should have access to data</p> <ul style="list-style-type: none"> • Training and guidance is provided to all employees that will be accessing and handling data (including more specifically, student data) • Background checks are performed on all employees • NDAs are signed by employees at the start of employment • All access to systems and data is revoked upon employment termination • All data stored electronically is kept secure by taking the following precautions: <ul style="list-style-type: none"> ▪ Use string passwords that should never be shared ▪ Servers are protected by security software and a firewall ▪ Backup data frequently ▪ Never disclose PII to unauthorized people within or outside of Capstone ▪ Routinely monitor systems for security breaches and attempts of inappropriate access

		<p>Measures to Protect Data: Capstone Digital Products use HTTPS connections to secure transmissions. A combination of firewalls, security keys, SSL certificates, and non-default username/password credentials secure data access. Additionally, the Buncee application has the following preemptive safeguards in place to identify potential threats, manage vulnerabilities and prevent intrusion:</p> <ul style="list-style-type: none">• All security patches are applied routinely• Server access logging is enabled on all servers• Fail2ban (an intrusion prevention software framework that protects servers from brute-force attacks) is installed on all servers and will automatically respond to illegitimate access attempts without intervention from engineers• Our database servers are not publicly accessible via the internet.• SSH key-based authentication is configured on all servers <p>Capstone Digital Products use HTTPS connections to secure transmissions. The HTTPS you see in the URL of your browser means when you go to the website, you're guaranteed to be getting the genuine website. With HTTPS in place, all interactions with Capstone Digital Products will be undecipherable by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic.</p> <p>Capstone Digital Products use SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees in PebbleGo Create and the Buncee products) is encrypted at rest. All passwords are encrypted using modern encryption technologies.</p> <p>Account information is stored in access-controlled VPCs operated by industry leading partners. All user information is stored</p>
--	--	---

		<p>redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.</p> <p>The Buncee application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption.</p>
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.	Officers and all employees of the Contractor who have access to student, teacher or principal data will receive ongoing training surrounding the Federal and State laws governing confidentiality of the data. This training will be performed and tracked through Curricula.
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.	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.

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>Capstone has implemented the following procedure to manage a data breach:</p> <p>Breach Investigation: A systematic approach to making a definitive determination as to whether a breach has taken place led by the VP of Information Technology and the Director of Business Systems Information Technology is created to investigate a potential breach. The response team will be tasked with isolating the affected systems, including taking the part or the entire site offline.</p> <p>Remediation Efforts: Upon identification, the response team will review the access logs and the monitoring software to figure out the cause of the breach. We will also consult experts at the cloud hosting service providers to help with the issue. Once the cause is identified, we will apply and monitor the fix and gradually bring the site online. The response team will also reset all session tokens for its users which will require that they log in again. Access tokens are valid for 24 hours in order to prevent unauthorized access.</p> <p>Internal Communication Plan: If it has been determined a breach occurred, the VP of Information Technology and the Director of Business Systems Information Technology will inform the President and CFO and explain what is being done to remediate the issue. After a solution has been implemented, an incident report detailing the cause, extent of damage, steps taken and recommendations to avoid in the future will be written by the response team and shared internally.</p> <p>Public Notification of Breach: After remediating the issue, the marketing team will work on informing all affected users about the breach and its severity. A brief statement will be shared via email explaining the incident and the solution will be sent within 72 hours after remediation is finalized. Additionally, the response team will monitor the dedicated email address privacy@capstonepub.com to address any follow-on questions.</p>
---	---	---

		<p>Capstone has adopted the following backup-and-restore process:</p> <ul style="list-style-type: none">• Use up-to-date images to spawn new servers. (if applicable also create a new load balancer)• Use the latest hot backup of the database to restore user data• Update the DNS records to point to the new load balancer• Verify the backup-and-restore process was successful <p>To protect against denial-of-service attack, Capstone has also established the following safeguards:</p> <ul style="list-style-type: none">• Robust alert & notification system in place to notify sudden traffic changes• Reverse proxy is used to prevent DDoS attack• Load-balancing is used to help distribute the load to multiple servers• Web Application Firewall (WAF) can be configured to block IP ranges• Notification system to alert instances of bot-like behavior from a user(s) <p>A typical incident response includes a combination of the following:</p> <p>Identification: The response team is initiated to determine the nature of the incident and what techniques and resources are required for the case.</p> <p>Containment: The team determines how far the problem has spread and contains the problem by disconnecting affected systems and devices to prevent further damage.</p> <p>Eradication: The team investigates to discover the origin of the incident. The root cause of the problem is determined and any traces of malicious code are removed.</p> <p>Recovery: Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for signs of weakness or recurrence.</p>
--	--	---

6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Contractor, upon written request of EA, will 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 and/or securely delete and destroy data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon written request of EA, Contractor shall dispose of or delete all Data obtained under the Contract when it is no longer needed for the purpose for which it was obtained, and transfer said data to EA or EA's designee within sixty (60) business days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Contractor acknowledges EA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by EA. Nothing in the Contract shall authorize Contractor to maintain Data obtained under the Contract beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to EA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been deidentified or placed in a separate Student account, pursuant to the other terms of the Contract. The EA may employ a "Request for Return or Deletion of Data" FORM. Upon receipt of a request from the EA, the Contractor will immediately provide the EA with any specified portion of the Data within sixty (60) business days of receipt of said request.
8	Outline how your data security and privacy program/practices <u>align</u> with the EA's applicable policies.	Contractor (Organization) will comply with the EA with whom it contracts and Education Law section 2-d by adhering to the following guidelines: <ul style="list-style-type: none"> • A student's personally identifiable information cannot be sold or released for any commercial purposes • Parents have the right to inspect and review the complete contents of their child's education record

		<ul style="list-style-type: none">• Contractor will follow state and federal laws which protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection will be in place when data is stored or transferred• Contractor will limit internal access to education records to those individuals that are determined to have legitimate educational interests• Except for authorized representatives of the Contractor to the extent they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order• Contractor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody• Contractor will use encryption technology to protect data while in motion or in its custody• Contractor will adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework <p>Contractor has also documented the following information regarding the receipt of student, teacher or principal data:</p> <ul style="list-style-type: none">• The exclusive purposes for which the student data or teacher or principal data will be used.• How the Contractor will ensure that the subcontractors, persons or entities that
--	--	---

		<p>the Contractor will share the student data or teacher or principal data with, will abide by data protection and security requirements.</p> <ul style="list-style-type: none"> • When the agreement expires and what happens to the student, teacher or principal data upon expiration of the agreement. • If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected. • Where the student, teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
9	<p>Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1.</p> <p>https://www.nist.gov/cyberframework/new-framework</p>	<p>Capstone’s data security and privacy practices align with the NIST Framework to manage cybersecurity risks for critical infrastructure. It allows us to identify different threats and vulnerabilities and customize our data security and privacy practices. By utilizing the core functions, Identify, Protect, Detect, Respond, and Recover, we are able to organize information and make risk management decisions that address threats and improve processes.</p> <ul style="list-style-type: none"> • Identify – Through a series of assessments, Capstone has developed an understanding of risk management. • Protect – Capstone has developed and implemented appropriate safeguards to ensure delivery of critical services. • Detect – Capstone has developed and implemented appropriate activities to identify the occurrence of a cybersecurity event. • Respond – Capstone has developed and implemented appropriate activities to take action regarding a detected cybersecurity incident.