

## New York

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between: West Genesee Central School District (the “Local Education Agency” or “LEA” or “New York Original LEA”) and Coughlan Companies, LLC Capstone (the “Provider”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the

Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312, applicable state privacy laws and regulations and

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in New York. Specifically, those are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

**WHEREAS**, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. Provider agrees to offer the LEA all the same terms and conditions found in the **MA-ME-NH-RI-VT-NDPA, Standard Version 1.0** Data Privacy Agreement between the Provider and **Orleans Southwest Supervisory Union** (“Originating LEA”) which is dated **4/6/22** (“Originating DPA”). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit “G” for New York, which will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of “General Offer of Privacy Terms” be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices.** All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA via e-mail transmission, or first-class mail, sent to the designated representatives below.


The designated representative for the Provider for this DPA is:

Name: Melissa Brodin Title: Director Contracts, Compliance, and Data Privacy  
Address: 1710 Roe Crest Drive North Mankato, MN 56003  
Phone: 800-747-4992 Email: mbrodin@capstonepub.com

The designated representative for the LEA for this DPA is:

Sean Fahey, Director of Accountability  
Phone: 315-487-6449  
Address: 300 Sanderson Drive Camillus, NY 13031  
Email: sfahey@westgenesee.org

**West Genesee Central School District**

By:   
Date: 11/12/24

Printed Name: Sean Fahey  
Title/Position:  
DPO

**Coughlan Companies, LLC dba Capstone**

By: Melissa Brodin  
Date: 11/08/2024

Printed Name: Melissa Brodin  
Title/Position: Director Contracts, Compliance, and Data Privacy

## **Exhibit "G"**

### **New York**

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".
6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such

Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a “**Directive for Disposition of Data**” form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in “**Exhibit D**”.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Contractor to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt

investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - i. The name and contact information of the reporting LEA subject to this section.
  - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
  - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
  - vi. The number of records affected, if known; and
  - vii. A description of the investigation undertaken so far; and
  - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- “Subprocessor” is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
  
- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **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
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt 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.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School

Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.

- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

-



**Exhibit "J"**  
**LEA Documents**

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

[https://sdpc.a4l.org/ny\\_dp\\_bor\\_url.php?districtID=12359](https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=12359)

**Exhibit "K"**  
**Provider Security Policy**

Provider's Data Security and Privacy Plan can be accessed at:

Attached

---



## Data Privacy Plan

### Purpose:

The purpose of this Data Privacy Plan is to describe how data is collected, handled and stored, and to ensure that Coughlan Companies, LLC dba Capstone does the following:

- Complies with local, state, federal and applicable international data protection laws and follows industry standard practices
- Protects the rights of employees, customers and partners
- Is transparent about how data is stored and processed
- Protects itself from risks associated with a data breach

### Product Scope:

This Data Privacy Plan applies to your access and use of the following digital software, educational platforms and tools offered by Capstone (collectively, the “Capstone Digital Products”):

- PebbleGo (including add-ons)
- PebbleGo Create
- Buncee (including all Buncee products)
- Capstone Interactive
- Capstone Connect

### Our Commitment:

Capstone is the nation’s leading educational publisher for digital solutions, children’s books, and literacy programs for school libraries and classrooms! Home of the award-winning PebbleGo research database and the easy-to-use creation tool Buncee, Capstone has a passion for creating inspired learning and intellectual curiosity in children.

Capstone takes privacy and the privacy of students very seriously. *PebbleGo*, *Capstone Interactive*, and *Capstone Connect* do not have individual student accounts, but rather a single building account shared by all educators and students. *PebbleGo Create*, *Buncee Classroom*, and *Buncee for Schools & Districts* do have individual educator and student accounts. Capstone does not collect, sell, rent, or otherwise provide personally identifiable information (“PII”) to any third parties for advertising or marketing purposes. Buncee participates in the [iKeepSafe COPPA Safe Harbor Certification](#) program, and Capstone is a signatory of the [Student Privacy Pledge](#). Protecting students online is one of Capstone’s top priority.



## **Plan Scope:**

This plan applies to the following:

- The leaders of Capstone
- All departments of Capstone
- All employees of Capstone
- All contractors and third-party operators working on behalf of Capstone

This plan applies to all data\*\* that is submitted to Capstone, more specifically personally identifiable information (“PII”), which may include:

- Names of individuals
- Email addresses
- Dates of birth
- Country/State
- Usernames
- Passwords
- District/School name
- IP addresses

\*\* Please note that under a *Buncee Classroom* plan, student sub-accounts can only be created by the subscriber (educator) of the plan, who is able to create unique usernames/passwords for their students. They are not asked to submit student email or birth data. Under a *PebbleGo Create* subscription or a *Buncee for Schools & Districts* subscription, classes, educator accounts, and student accounts are created by syncing the School/District’s roster data through integrations made available through the Buncee application, or by manually uploading the applicable roster data in .csv format. Furthermore, all passwords created or changed after 02/2017 are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm.

## **Responsibilities:**

Everyone working for or with Capstone has responsibility for ensuring that data is collected, stored and handled properly. Each team that handles personal data will ensure that it does so in line with Capstone’s Privacy Policy and Data Privacy Plan. All Capstone employees receive Data Security Training, and the manager of each team is responsible for the following:

- Risk and Contracts/HR:
  - Reviewing all data protection procedures
  - Organizing data protection and policy training and guidance
  - Handling data protection questions
  - Handling access requests from districts, schools and individuals
  - Administration of any contracts and agreements pertaining to Capstone’s data protection procedures, including but not limited to Data Privacy Agreements and third-party Data Processing Agreements



- Evaluating third-party services to ensure that they are in compliance with Capstone's Privacy Policy and Data Privacy Plan
- Reviewing current and new data privacy laws and regulations to ensure compliance
- Management of deletion requests
- Development:
  - Ensuring all systems, services and equipment used to store data meet acceptable security standards
  - Performing routine checks and scans to ensure security measures are functioning correctly
  - Responsible for deletion of PII when termination is requested by a district/school
- Marketing/Sales:
  - Partner with Operations and Development to ensure marketing initiatives abide by Capstone's Privacy Policy and Data Privacy Plan
  - Evaluating third-party services to ensure that they are in compliance with Capstone's data collection and protection policies
  - Partner with Operations and Development to understand current and new data privacy laws and regulations specific to marketing and sales initiatives

### **Employee Guidelines:**

- Only those who need it to perform their duties should have access to data
- 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:
  - Use strong 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

### **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 following preemptive safeguards are 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 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.

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 Projects in PebbleGo Create and the Buncee products) is encrypted at rest. All passwords are encrypted using modern encryption technologies.

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.

Capstone Digital Products are hosted on cloud servers managed by Amazon Web Services, which is 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.

You can learn more about the security practices of the cloud hosting providers here: [Overview of Security Processes at AWS \(https://aws.amazon.com/whitepapers/overview-of-security-processes/\)](https://aws.amazon.com/whitepapers/overview-of-security-processes/).

### **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.

Capstone Digital Products do 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.

### **Data Breach, Incident Investigation and Response:**

Capstone has implemented the following procedure to manage a data breach:

*Breach Investigation:* A systematic approach to making a definitive determination as to whether a breach has taken place will be led by Capstone's Incident Response Team ("Response Team") 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.

*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.

*Internal Communication Plan:* If it has been determined a breach occurred, the Response Team will inform the CEO 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.

*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](mailto:privacy@capstonepub.com) to address any follow-on questions.

Capstone has adopted the following backup-and-restore process:

- 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



To protect against denial-of-service attack, Capstone has also established the following safeguards:

- 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)

A typical incident response includes a combination of the following:

*Identification:* The Response Team is initiated to determine the nature of the incident and what techniques and resources are required for the case.

*Containment:* The team determines how far the problem has spread and contains the problem by disconnecting affected systems and devices to prevent further damage.

*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.

*Recovery:* Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for signs of weakness or recurrence.

### **Data Collection and Use:**

Data is collected in order to administer your account with us and improve and customize the service we provide to you. We do not sell, rent, or otherwise provide your personally identifiable information to any third parties for marketing or advertising purposes. We will not collect, use, or share such information for any purposes beyond educational/school purposes, or as authorized by the district/school, educator, student, or parent.

Under a Buncee Classroom subscription, educator accounts require the completion of the registration form which requests name, email address, gender, date of birth, country, state (if applicable), name of school, unique username, and password. Student sub-accounts and their unique usernames/passwords can only be created manually, by CSV upload, or by class code issued by the subscriber (educator) of the *Buncee Classroom* plan. Under a *PebbleGo Create* subscription or a *Buncee for Schools & Districts* subscription, classes, educator accounts, and student accounts are created by syncing the School/District's roster data through integrations made available through the Buncee application, or by manually uploading the applicable roster data in .csv format.

The purpose of data processing is to allow Capstone to provide the requested Services to the District and perform the obligations under our Agreement. More specifically, the purpose of processing data is to enable school oversight and ensure appropriate structure and interaction within a school account. 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. Capstone requires data capture and use for the following reasons:

- 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 differentiate instruction, and monitor and assess student progress
- To allow subscribers to monitor and safeguard student welfare
- 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 subaccounts)

Capstone does not sell, rent, or otherwise provide personally identifiable information to any third parties for marketing or advertising purposes. Additionally, Capstone 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 Capstone by state and federal laws and regulations.

### **Access and Disposal:**

A parent, eligible student, educator or principal may challenge the accuracy of the data that is collected. They are entitled to ask the following:

- What information Capstone holds about them and why
- If there is data that is inaccurate that may need to be corrected
- How they can gain access to that information
- How they can keep it up to date
- How Capstone is protecting their data

All requests should be made via email at [privacy@capstonepub.com](mailto:privacy@capstonepub.com). The Data Privacy Administrator will then verify the identity of anyone making a request before handing over any information.

Account information will be retained by Capstone only to the extent necessary to fulfill its obligations under the Agreement and Capstone may take steps to destroy such data when it determines, in its discretion, that the data is no longer needed for the purposes for which it was disclosed. In any event, Capstone reserves the right to delete and destroy account data, including but not limited to User Content and information from or related to Education Records, thirty-six (36) months from the date of the earliest to occur of the following: (i) termination or expiration of this Agreement, (ii) your failure to pay fees in accordance with the terms of this Agreement, or (iii) a user account shows no user activity for a period of six (6) months. Capstone may retain copies of data related to your use of the Capstone Digital Products, including User Content, to the extent it deems is necessary to comply with applicable laws, resolve disputes, enforce its legal



agreements or policies, or verify and validate any requests made by you. It is the educator's and/or the school/district's responsibility to maintain and retain any student information, including Education Records, pursuant to and in accordance with any laws, rules, regulations, policies, or obligations applicable to you and/or your School/District.

### **Individual Rights:**

Individual Rights are the rights that individuals (otherwise known as data subjects) have to access, correct, export, and delete personal data that companies hold about them. Capstone has built mechanisms into our products and services so you can have more visibility into what personal data we have collected and make choices about that data. To find out more about how Capstone processes and protects your personal data, you can access our Privacy Policies [here](#).

You can view and clear your browsing and search history within your browser dashboard. You can view and update your profile information by either signing into your individual account or reaching out to the administrator of your school or district account. If you utilize one of Capstone's creation platforms and have personal content that you want to view or download, you can sign into your account and utilize the tools to do so within those products. To opt-out or unsubscribe from marketing emails, click the "Unsubscribe" button directly within the email you received.

In addition, you have the following options available to exercise your Individual Rights:

- For Customers in any jurisdiction, please use [this form](#)
- For Cooperative Educational Services in any jurisdiction, please use [this form](#)
- For Employees, Former Employees, Job Applicants, or Contractors in California, the European Economic Area (EEA), European Union (EU), United Kingdom, or Switzerland please use [this form](#)
- Email us at [privacy@capstonepub.com](mailto:privacy@capstonepub.com)

Please Note: Students or teachers within a school or district account should contact the school or district administrator to submit a request

### **Compliance:**

***Children's Online Privacy Protection Act (COPPA)***, per <http://www.coppa.org/coppa.htm?>

Capstone is a COPPA Compliant Platform, and is committed to protecting the privacy of the children who access this platform. The Buncee platform participates in the iKeepSafe COPPA Safe Harbor Certification program, which ensures that practices surrounding the collection, use, maintenance, and disclosure of personal information from children under the age of 13 are consistent with principles and requirements of the Children's Online Privacy Protection Act (COPPA). After undergoing a rigorous review of our data security and privacy procedures, [iKeepSafe](#), which operates one of the six safe harbor programs approved by the FTC, awarded the Buncee platform the iKeepSafe COPPA Safe Harbor Certification. This certification makes it easy for parents and schools to identify that the Buncee platform is compliant with COPPA.



**Family Educational Rights and Privacy Act (FERPA), per**

<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?>

Capstone is committed to maintaining the confidentiality of student education records. We have developed, implemented, and will maintain technical and physical security measures in order to safeguard student records. Capstone does not collect information including but not limited to, the following: personnel records, social security numbers, credit card numbers, expiration dates, PINs, card security codes, financial profiles, bank routing numbers, medical data, student identifiers, student gender, student grade, race/ethnicity, IDEA Indicator, limited English proficiency status, section 504 status, and Title I Targeted Assistance Participation. Further, we do not sell, rent, or otherwise provide any personally identifiable information to any third parties for marketing purposes.

**Student Online Personal Information Protection Act (SOPIPA), per**

[https://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=201320140SB1177](https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177)

Capstone is committed to protecting the privacy of students, and therefore does not share/use student data for targeted advertising on students for a non-educational purpose. We do not sell, rent, or otherwise provide personally identifiable information to any third parties for marketing or advertising purposes. Capstone also adheres to deletion guidelines addressed by SOPIPA and will delete a student's information at the written request of the school/district.

**Children's Internet Protection Act (CIPA)** - Capstone addresses the Children's Internet Protection Act through the implementation of our own safe search parameters for all users that are performing web searches from within the Buncee platform or mobile application. All searches performed from within the Buncee platform are internally filtered in order to protect children from harmful online content.

**Privacy Act** - Capstone does not collect information including, but not limited to, the following: personnel records, social security numbers, credit card numbers, expiration dates, PINs, card security codes, financial profiles, bank routing numbers, medical data, student identifiers, student gender, student grade, race/ethnicity, IDEA Indicator, limited English proficiency status, section 504 status, and Title I Targeted Assistance Participation. Further, we do not sell, rent, or otherwise provide any personally identifiable information to any third parties for marketing purposes. Student sub-accounts created by a *PebbleGo Create* subscriber, *Buncee Classroom* subscriber or a *Buncee for Schools & Districts* subscriber are private by default and will only be visible to the subscriber, not to other Users. User data is stored in secure and managed cloud servers, accessible only to the internal team via secure shell. User data backups are performed routinely and securely backed on the cloud. Stale data copies are permanently purged. Furthermore, sensitive data like passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm.

**Protection of Pupil Rights Amendment, per**

<https://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html>



Capstone does not perform surveys, analyses, or evaluations which may reveal personal information about minor students. Furthermore, for accounts known to be student accounts, we do not send service or promotional communications from Capstone.

***EU General Data Protection Regulation (GDPR)***, per

[https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)

Capstone is compliant with the EU General Data Protection Regulation (GDPR), and provides users with the following data protection rights if their Personal Information is protected by the EU General Data Protection Regulation (GDPR):

- a. Right of access, correction, and portability -- The right to access, correct, update, or delete your Personal Information, as well as the right to transfer data from one service provider to another.
- b. Right to be informed -- The right to be informed before data is gathered. You must opt in for data to be gathered, or to receive marketing updates and emails.
- c. Right to be forgotten -- The right to request to have data deleted if you are no longer a customer or wish to withdraw parental consent.
- d. Right to restrict processing -- The right to contest the accuracy of your personal information and maintain that while your information can remain intact, your data should not be used for processing.
- e. Right to object -- The right to object to the processing of your personal information for direct marketing purposes.
- f. Right to report -- The right to make a complaint to the relevant Supervisory Authority. A list of Supervisory Authorities can be found here: <https://dataprivacymanager.net/list-of-eu-data-protection-supervisory-authorities-gdpr/>

***California Consumer Privacy Act (CCPA)***, per <https://oag.ca.gov/privacy/ccpa>

Capstone is compliant with the California Consumer Privacy Act (CCPA) and provides users with the following data protection rights if their Personal Information is protected by the California Consumer Privacy Act (CCPA):

- The [right to know](#) about the personal information a business collects about them and how it is used and shared;
- The [right to delete](#) personal information collected from them (with some exceptions);
- The [right to opt-out](#) of the sale of their personal information; and
- The [right to non-discrimination](#) for exercising their CCPA rights.

***Personal Information Protection and Electronic Documents Act (PIPEDA)***, per

<https://www.priv.gc.ca/en/>



Capstone follows the [10 fair information principles](#) to protect personal information, which are set out in Schedule 1 of PIPEDA. By following these principles, we build trust in our business and in the digital economy.

The principles are:

1. [Accountability](#)
2. [Identifying Purposes](#)
3. [Consent](#)
4. [Limiting Collection](#)
5. [Limiting Use, Disclosure, and Retention](#)
6. [Accuracy](#)
7. [Safeguards](#)
8. [Openness](#)
9. [Individual Access](#)
10. [Challenging Compliance](#)

***NYSED Law 2-d, “The Parent Bill of Rights for Student Data Privacy Act”***, per <https://www.nysenate.gov/legislation/laws/EDN/2-D>

Capstone is compliant with NYSED Law 2-D. We do not sell or release a student's personally identifiable information for any commercial purposes, and give parents the right to inspect and review the complete contents of their child's records. Capstone is in compliance with the five criteria the law requires, and provides users with the following data protection rights if their Personal Information is protected by NYSED Law 2-D:

- Purpose: the exclusive purpose for which the data will be used
- Protection: how Capstone ensures that contractors, persons or entities that the third party product shared student, principal or educator data with, if any, will abide by data protection and security requirements employed by Capstone
- Disposal: how student, principal or educator data is disposed after the expiration of the agreement with the district
- Correction: how a parent, eligible student, educator or principal may challenge the accuracy of the data that is collected
- Location: where the student, principal or educator data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected

For more information about Capstone's commitment to protecting you and your data online, you can access our Privacy Policies here: <https://www.capstonepub.com/support/privacy-central>

# NY\_West Genesee\_Addition to Orleans Southwest Supervisory\_VendorSigned

Final Audit Report

2024-11-12

Created:	2024-11-11
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAeGfxjckLsg7leR9SD2ChCDr_6WzHKXBT

## "NY\_West Genesee\_Addition to Orleans Southwest Supervisory\_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2024-11-11 - 7:34:27 PM GMT
-  Document emailed to Sean Fahey (sfahey@westgenesee.org) for signature  
2024-11-11 - 7:34:34 PM GMT
-  Email viewed by Sean Fahey (sfahey@westgenesee.org)  
2024-11-12 - 2:11:36 PM GMT
-  Document e-signed by Sean Fahey (sfahey@westgenesee.org)  
Signature Date: 2024-11-12 - 2:12:30 PM GMT - Time Source: server
-  Agreement completed.  
2024-11-12 - 2:12:30 PM GMT

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

**MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND, AND VERMONT**

**MA-ME-NH-RI-VT-NDPA, Standard Version 1.0**

**ORLEANS SOUTHWEST SUPERVISORY UNION**

**and**

**CAPSTONE**

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Orleans Southwest Supervisory Union, located at 157 Daniels Road, Hardwick, VT 05843 (the “**Local Education Agency**” or “**LEA**”) and Capstone, located at 1710 Roe Crest Drive, North Mankato, MN 56003 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.



The designated representative for the Provider for this DPA is:

Name: Melissa Brodin Title: Senior Risk & Contracts Officer

Address: 1710 Roe Crest Drive, North Mankato, MN 56003

Phone: (800) 747-4992

Email: mbrodin@capstonepub.com

The designated representative for the LEA for this DPA is:

David Martin, Director of Tech & Communications  
Orleans Southwest Supervisory Union  
157 Daniels Road, Hardwick VT 05843  
802.472.2906  
dmartin@ossu.org

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**ORLEANS SOUTHWEST SUPERVISORY UNION**

By: *Jack Bassett*  
Jack Bassett (Apr 7, 2022 10:13 EDT)

Date: 04/06/2022

Printed Name: Jack Bassett

Title/Position: Tech Support

**CAPSTONE**

DocuSigned by:  
By: *Melissa Brodin*  
7F5901D797804C5...

Date: 04/05/2022

Printed Name: Melissa Brodin

Title/Position: Senior Risk & Contracts Officer

## **STANDARD CLAUSES**

Version 1.0

### **ARTICLE I: PURPOSE AND SCOPE**

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

- Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
- Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## **ARTICLE VI: GENERAL OFFER OF TERMS**

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## **ARTICLE VII: MISCELLANEOUS**

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## EXHIBIT "A"

### DESCRIPTION OF SERVICES

This Exhibit "A" applies to the following educational platforms and tools offered by Capstone:

Product Line A, referred to as Line A on Exhibit "B", Schedule of Data  
PebbleGo (Including PebbleGo Next, PebbleGo Spanish, Read More)  
Capstone Interactive  
Capstone Connect

Product Line B, referred to as Line B on Exhibit "B", Schedule of Data  
PebbleGo Create with Buncee  
Buncee

**PebbleGo.** Capstone's unique database of educational curriculum with informational articles, ready-made activities, and literacy supports. PebbleGo Next incorporates a streamlined interface, animated highlighting, educational videos and games, and encompassing activities that teach students how to cite articles, create reports, and share what they've learned. PebbleGo Spanish provides Spanish modules, while Read More provides two read-aloud eBooks connected to each article in the PebbleGo Animals and PebbleGo Science modules. PebbleGo does not have individual student accounts, but rather a single building account shared by all students and educators which can be configured to support IP authentication. PebbleGo does not collect Student Identifiers such as Student Username, Student Password, Student Name, or Student Generated Content.

**Capstone Interactive.** Over 5,000 titles of interactive eBooks designed specifically for PreK-Grade 5. This product does not have individual student accounts, but rather a single building account shared by all students and educators which can be configured to support IP authentication. Capstone Interactive does not collect Student Identifiers such as Student Username, Student Password, Student Name, or Student Generated Content.

**Capstone Connect.** Capstone's large online source of K-5 eBook bundles, nonfiction articles, and instructional support united by a single search. This product does not have individual student accounts, but rather a single building account shared by all educators which can be configured to support IP authentication. Capstone Connect is a platform for educators, and therefore does not collect Student Identifiers such as Student Username, Student Password, Student Name, or Student Generated Content.

**PebbleGo Create with Buncee.** As an add-on to PebbleGo, PebbleGo Create with Buncee is a creation tool that allows students, educators, and administrators to create and publish original and authentic content. This product does 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.

**Buncee.** A K-12 creation and communication tool that allows students, educators, and administrators to create and publish original and authentic content. This platform is delivered through Buncee for Schools & Districts or Buncee Classroom. These products do have individual student accounts. Buncee for Schools & Districts accounts can be created by syncing Google Classroom roster data or Microsoft 365 roster data with Buncee, or manual upload via CSV. Buncee Classroom accounts can be created by manual entry or manual upload via CSV.



**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X, Line A, Line B
	Other application technology meta data-Please specify:	X, Browser Agent, Line A, Line B
Application Use Statistics	Meta data on user interaction with application	X, De-identified, Line A, Line B
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	X, Line B
	Student app username	X, Line B
	Student app passwords	X, Encrypted, Line B
Student Name	First and/or Last	X, Full name not required, Line B
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X, Within their creations, Line B
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used by Your System
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

## **EXHIBIT "C"** **DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Student Generated Content:** The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities,

socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G"**  
**Massachusetts**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.



**EXHIBIT "G"**

**Maine**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
  - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
  - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
  - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

**EXHIBIT "G"**  
**Rhode Island**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
  - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

**EXHIBIT "G"**  
**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "1"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts for Student and Teacher Data;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
  - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
  - (10) Perform maintenance on organizational systems;
  - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
  - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
  - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
  - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
  - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
  - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

<b>EXHIBIT "1" – TEACHER DATA</b>		
<b>Category of Data</b>	<b>Elements</b>	<b>Check if used by your system</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X, Line A, Line B
	Other application technology meta data-Please specify:	X, Browser Agent, Line A, Line B
Application Use Statistics	Meta data on user interaction with application	X, Line A, Line B
Communications	Online communications that are captured (emails, blog entries)	X, Line A, Line B
Demographics	Date of Birth	X, Line B
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X, Line B
	Teacher app username	X, Line B
	Teacher app passwords	X, Encrypted, Line B
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	X, Line A, Line B
Teacher work	Teacher generated content; writing, pictures etc.	X, Within their creations, Line B
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	



**EXHIBIT "G"**  
**Vermont**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.








# PebbleGo\_Orleans\_VendorSigned

Final Audit Report

2022-04-07

Created:	2022-04-07
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA_ZLudC4t8IEpNZhJ8MTEHPUSUVpwUahQ

## "PebbleGo\_Orleans\_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2022-04-07 - 2:09:16 PM GMT- IP address: 74.102.102.44
-  Document emailed to Jack Bassett (jbassett@ossu.org) for signature  
2022-04-07 - 2:10:07 PM GMT
-  Email viewed by Jack Bassett (jbassett@ossu.org)  
2022-04-07 - 2:10:09 PM GMT- IP address: 66.249.92.32
-  Document e-signed by Jack Bassett (jbassett@ossu.org)  
Signature Date: 2022-04-07 - 2:13:27 PM GMT - Time Source: server- IP address: 71.161.109.46
-  Agreement completed.  
2022-04-07 - 2:13:27 PM GMT