EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Coughlan Companies, LLC dba Capstone (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Shoreham-Wading River Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District 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.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;
b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
e. Where the student data or teacher or principal 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, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall immediately notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of

the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Mr. Gerard Poole
Shoreham-Wading River Central School District
250B Rt. 25A
Shoreham, NY 11786

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: **Coughlan Companies, LLC dba Capstone**

Signature: Melissa Brodin **Date:** **05/23/2025**

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

EXHIBIT "A"

Shoreham-Wading River Central School District
Parents' Bill of Rights

Parents and guardians of students attending or seeking to enroll in the Shoreham-Wading River CSD are advised that they have the following rights with regard to student data under New York State Education Law.

1. A student's personally identifiable information will not be released or sold by the District for any commercial purposes.

2. A parent or guardian has the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third Party contractors are required to employ technology, safeguards, and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by New York State is available for public review at https://www.nysed.gov/data-privacy-security/student-data-inventoryor by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. 89 Washington Avenue Albany, NY 12234

   Complaints should be addressed to:

   Alan Meinster, Assistant Superintendent for Curriculum, Instruction, and Assessment; DPO
   250B Route 25A
   Shoreham, NY 11786
   (631) 821-8100
   Or with NYSED
   Chief Privacy Officer
   New York State Education Department
   Email: Privacy@nysed.gov

6. This Bill of Rights will be included with every contract entered by the District with an outside contractor if the contractor will receive student, teacher, or principal data. This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student, teacher, or principal data, including the exclusive purpose (s) for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.

7. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

8. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, the District will notify the public via written notice, electronic notice through the District's electronic communication platform, or Telephone notification.

9. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

10. Parents may access the State Education Department's Parent's Bill of Rights at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Contractor: **Coughlan Companies, LLC dba Capstone**

Signature: Melissa Brodin **Date:** **05/23/2025**

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

EXHIBIT "B"
Contractor's Supplemental Information

Name of Contractor	Coughlan Companies, LLC dba Capstone
Description of the purpose(s) for which Contractor will receive/access PII	Contractor will receive/access PII to provide the requested Services to the District and perform the obligations under the Contract.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: 05/23/2025 Agreement End Date: 06/30/2027
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by State and federal laws and regulations, and the Agreement. (check applicable option): ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected (check all that apply): ☒ Using a cloud or infrastructure owned and hosted by a third-party. ☐ Using Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

Contractor: **Coughlan Companies, LLC dba Capstone**

Signature: Melissa Brodin **Date:** **05/23/2025**

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

EXHIBIT "C"
Contractor's Data Security & Privacy Plan

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

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/).

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 President 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 after remediation is finalized. Additionally, the Response Team will monitor the dedicated email address 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. 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

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.legislature.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
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