## TEXAS DATA PRIVACY AGREEMENT/ADDEDNUM TO SERVICE AGREEMENT

This Texas Data Privacy Agreement ("DPA:) is entered into by and between the Wichita Falls Independent School District (hereinafter referred to as "LEA) and Buncee LLC (hereinafter referred to as "Operator"). The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS,** the Operator has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated 10/30/2019 titled Buncee-Wichita Falls DPA ("Service Agreement"); and

**WHEREAS,** in order to provide the Services described in the Service Agreement, the Operator may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

**WHEREAS,** the documents and data transferred from LEAs and created by the Operator's Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

**WHEREAS,** this Agreement complies with Texas and Federal laws; and

**WHEREAS,** the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

**WHEREAS,** the Operator may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

## ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** For Operator to provide services to the LEA it may become necessary for the LEA to share certain Data related to the LEA's students, employees, business practices, and/or intellectual property. This agreement describes responsibilities to protect Data between the LEA and Operator.

2. **Nature of Services Provided.** The Operator has agreed to provide the following digital educational services as set out in the Service Agreement. – EXHIBIT A

3. **Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "A"

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Exhibit "B". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Data Property of LEA**. All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Operator shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Data notwithstanding the above. Operator may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than five (5) days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA in a reasonable time not to exceed one (1) week, who will follow the necessary and proper procedures regarding the requested information.

3. **Access to Student Generated Content**. Operator shall, at the request of the LEA, make Pupil Generated Content available in a readily accessible format.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within one (1) business day) redirect the Third Party to request the data directly from the LEA. Operator shall promptly notify the LEA in advance of a compelled disclosure to a Third Party and provide a copy of the request no later than ten (10) business days before disclosure is required. The Operator will not use, disclose, compile, transfer, sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof.

   Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.

5. **No Unauthorized Use**. Operator shall not use Data for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors.** Operator shall either (1) enter into written agreements with all Subprocessors, listed in Exhibit D, performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Data in a manner the same or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and

employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting the acts of omissions of its Subprocessors/subcontractors.

## ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other applicable Federal and Texas privacy statutes and legal requirements.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under 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, and determine whether Operator qualifies as a school official.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification.** LEA shall notify Operator promptly of any known or suspected unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

## ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance.** The Parties expect and anticipate that Operator may receive personally identifiable information in education records from the District only as an incident of service or training that Operator provides to the LEA pursuant to this Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes quoted in this DPA. The Parties agree that Operator is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Operator also acknowledges and agrees that it shall not make any re-disclosure of any Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Data, without the express written consent of the LEA.

3. **Employee Obligation.** Operator shall require all its employees, agents, and Subprocessors (if any) who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and maintain an appropriate confidentiality agreement from each of its employees, agents, or Subprocessors (if any) with access to Data pursuant to the Service Agreement.

4. **No Disclosure.** De-identified information may be used by the Operator for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify de-identified Data and not to transfer de-identified 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 LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Operator to maintain Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been de-identified or otherwise downloaded or transferred by the LEA or an authorized user, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" Form, a copy of which is attached hereto as Exhibit "C"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within three (3) calendar days of receipt of said request.

6. **Advertising Prohibition.** Operator is prohibited from using or selling Data to (a) market or advertise to the LEA's students, families/guardians, or the LEA's employees; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by an Operator; (c) develop a profile of a student, family member/guardian or group, or an LEA employee for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations unless the LEA has provided written notice to the Operator to cease such personalized learning recommendations.

7. **Access to Data.** Operator shall make Data in the possession of the Operator available to the LEA immediately (not to exceed one (1) business day) upon request by the LEA.

## ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. Operator may further detail its security programs and measures in Exhibit "D" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access.** Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level suggested by Article 4.3 of NIST 800-63-3. Operator shall only provide access to Data to employees or contractors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.

b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

c. **Employee Training.** The Operator shall provide periodic security training to those of its employees who operate or have access to the system. Further, Operator shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

d. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

e. **Security Coordinator.** Operator shall provide the name and contact information of Operator's Security Coordinator for the Data received pursuant to the Service Agreement, pursuant to Exhibit D.

f. **Subprocessors Bound.** Operator shall enter into written agreements whereby Subprocessors, listed in Exhibit D, agree to secure and protect Data in a manner consistent with the terms of this Article V. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

g. **Periodic Risk Assessment.** Operator further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA with the results of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DPA.

h. **Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of Data or any portion thereof.

i. **Audits.** Upon receipt of a request from the LEA, the Operator will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Data. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA.

j. **Data Transfer.** Operator agrees that all data will be transferred using secure FTP and/or physical delivery, at the LEA's discretion.

2. **Data Breach.** When Operator reasonably suspects and/or becomes aware of a disclosure or security breach concerning any Data covered by this Agreement, Operator shall immediately notify the District and take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible.

   a. Subject to the following requirements, the Operator shall provide a security breach notification to the LEA.

      i. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

      ii. The security breach notification described above in section 2(a)(i) shall include, at a minimum, the following information:

         1. The name and contact information of the reporting LEA subject to this section.
         2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
         3. 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.
         4. 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.
         5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

      iii. The security breach notification must include at least:

         1. Information about what the Operator has done to protect individuals whose information has been breached.
         2. Advice on steps that the person whose information has been breached may take to protect himself or herself.
         3. Information about the steps the Operator has taken to cure the breach and the estimated timeframe for such cure.

   b. Operator agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   c. Operator 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 Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

d. At the request and with the assistance of LEA, Operator shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsection (a) above.

e. The Parties agree that any breach of the privacy and/or confidentiality obligation set forth in the DPA may, at the LEA's discretion, result in the LEA immediately terminating the Service Agreement and any other agreement for goods and services with Operator. Termination does not absolve the Operator's responsibility to comply with the disposition procedures of Data.

f. Operator shall timely notify law enforcement as appropriate of any breach or suspected breach.

3. **Data "As-is."** Operator agrees and understands that the LEA will provide data to the Operator "as is" and "as available." The LEA is not under any obligation to modify the data, including but not limited to creating any different student identification numbers or alias.

## ARTICLE VI: MISCELLANEOUS

1. **Term.** The Operator shall be bound by this DPA for the duration of the Service Agreement or so long as the Operator maintains any Data, whichever is later. Notwithstanding the foregoing, Operator agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **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.

3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.

4. **Priority of Agreements.** This DPA shall govern the treatment of 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, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or first class mail, postage prepaid, sent to the designated representatives and at the address provided below:

The designated representative and mailing address for the Operator for this Agreement is:

Name: Claire Cucchi
Position: Chief Operations Officer
Mailing Address: Buncee LLC
PO Box 429, Speonk NY 11972

The designated representative and mailing address for the LEA for this Agreement is:

Name: Timothy Sherrod
Position: Chief Financial Officer
Mailing Address: Wichita Falls ISD
PO Box 97533
Wichita Falls, TX 76307

6. **Entire Agreement.** This DPA constitutes 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 an authorized representative from 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.

7. **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.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.

10. **Waiver.** Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees,

and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

11. **Assignment.** None of the parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of an authorized representative of the other party to this DPA.

## ARTICLE VII: MISCELLANEOUS PROVISIONS

12. **Venue.** Both parties agree that venue for any litigation arising from this contract shall lie in state or federal court having jurisdiction over Travis County, Texas.

13. **Notifications of Amendments to Policy.** Operator shall not change how Data is collected, used, or shared under the terms of the DPA and corresponding Service Agreement in any way without advance notice to and written consent by an authorized representative of the LEA. Operator shall provide notice to the LEA of any proposed change to its Terms of Use, Privacy Policy, and/or any similar policies/procedures thirty (30) days prior to the implementation of any such change. This agreement supersedes online Terms of Use and Conditions.

14. **Severability.** The provisions of this DPA and Service Agreement are severable. If a court of competent jurisdiction determines that any portion of this DPA and/or Service Agreement is invalid or unenforceable, the court's ruling will not affect the validity or enforceability of the other provisions of the DPA or Service Agreement.

15. **Insurance.** Operator shall take out and maintain, at its expense, until termination of the Service Agreement, at least the following insurance with an appropriately licensed insurance company in the state of Texas:

| Insurance Type | Amount Required |
|---|---|
| Commercial General Liability | $1,000,000 |
| BI & PD - each occurrence | $ 100,000 |
| BI & PD – aggregate | $ 300,000 |
| Medical Expenses – any one person | $ 10,000 |
| Personal & Adv Injury – each occurrence | $1,000,000 |
| Commercial Auto Liability<br>-- All owned/non-owned/hired combined single limits | $1,000,000 |
| Excess/Umbrella Liability | $1,000,000 |
| Workers' Compensation | Statutory Limits |
| Errors & Omissions Coverage | $7,000,000 |
| Cyber Liability Coverage | $1,000,000 |

Operator shall have the LEA named as additional insured under the above insurance policy obtained by Operator. Such additional insured status shall be procured and evidenced by an additional insured endorsement on the policy and certificate of insurance.

Operator represents that it is not an employee of the LEA and that it has or will follow Texas statutory guidelines regarding workers compensation. Operator shall require all subcontractors performing any work to maintain coverage as specified herein.

16. **Data Storage.** Operator acknowledges and agrees that all electronic data and records will not be shipped, stored, transferred, or exported outside the United States, including any backups or copies, without prior written consent from an authorized representative of the LEA.

17. **Notification of Criminal History.** A person or business entity that enters into a contract with a Texas public school district, such as the LEA, must give advance notice to the LEA if the person or an owner or operator of the business entity has been convicted of a felony. Pursuant to the Texas Education Code §22.0834 and the Texas Government Code §411.082, Operator will, at least annually, obtain criminal history record information that relates to an employee, applicant, or agent of Operator, if the person has or will have continuing duties related to the LEA, and the duties are or will be performed on the LEA's property or at another location where students are regularly present. Operator shall assume all expenses associated with the background checks, and shall immediately remove any employee or agent who was convicted of a felony or a misdemeanor involving moral turpitude from the LEA's property or other location where students are regularly present. Licensee shall determine what constitutes "moral turpitude" or "a location where students are regularly present." Operator understands that failure to comply with the requirements of this section may be grounds for termination of the Service Agreement.

    Operator further agrees that employees who will have access to raw data that has not been disaggregated will also undergo criminal background checks at least annually. Operator shall assume all expenses associated with the background checks, and shall immediately remove any employee or agent who was convicted of a felony or a misdemeanor involving moral turpitude from the LEA's property or other location where students are regularly present.

18. **Compliance with Texas Government Code Chapter 2270; Prohibition on Contract with Companies that Boycott Israel.** Operator represents and warrants that it does not boycott Israel and will not boycott Israel during the Term of the Service Agreement.

*[Signature Page Follows]*

**IN WITNESS WHEREOF,** the parties have executed this Texas Data Privacy Agreement as of the date of the last signature noted below.

Authorized Representative of LEA:

BY: Timothy Sherrod Date: 10/22/2019

Printed Name: Timothy Sherrod Title/Position: Chief Financial Officer

Authorized Representative of Operator:

BY: Date: 10/30/2019

Printed Name: Claire Cucchi Title/Position: Chief Operations Officer

**EXHIBIT "A"**

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

Buncee is an award-winning creation and communication tool for students, teachers and administrators. Our all-in-one technology empowers all users to easily create and share visual representations of content. Buncee is used in classrooms to help students of all ages and abilities visualize and voice their thoughts and ideas, as well as to document their mastery of learning standards in a fun, engaging way! With a wealth of opportunities for creating and sharing, students are empowered with choices for how they would like to document and demonstrate their knowledge acquisition. Given the breadth of media and creation features available, our tool not only benefits students, but is also actively used by educators and administrators. Educators use the tool to develop visually engaging and interactive classroom content that supports learning and instruction in countless ways. School and district administrators lean on Buncee to brand and communicate district successes, as well as develop community outreach materials. With unlimited possibilities for bringing learning to life, Buncee is a powerful solution for all users across the schoolhouse.

Our creation and communication tool is delivered through 2 main product plans:
Buncee Classroom: Includes the Buncee creation and communication tool, sharing functionalities, as well as the ability for educators to create student accounts to extend Buncee's creation experience to their students. Additional features include access to the classroom dashboard, the templates library, Ideas Lab, as well as the ability to earn badges. (Classroom Lite: 50 Students max, Classroom Plus: 150 students max)

Buncee for Schools and Districts: Our enterprise build includes everything in a Buncee Classroom Plan, in addition to unlimited students, private access to Buncee's Resource Library, the ability to customize your organization's own templates and graphics library; and an administrative management dashboard to monitor user permissions and privacies and synchronize rosters.

# EXHIBIT "A"

## 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. | ☑ |
| | Other application technology meta data-Please specify: Browser Agent | ☑ |
| Application Use Statistics | Meta data on user interaction with application de-identified | ☑ |
| Assessment | Standardized test scores | □ |
| | Observation data | □ |
| | Other assessment data – Please specify: | □ |
| Attendance | Student school (daily) attendance data | □ |
| | Student class attendance data | □ |
| Communications | Online communication that are captured (emails, blogs entries) | □ |
| Conduct | Conduct or behavioral data | □ |
| Demographics | Date of Birth | □ |
| | Place of Birth | □ |
| | Gender | □ |
| | Ethnicity or race | □ |
| | Language information (native, preferred or primary language spoken by student) | □ |
| Enrollment | Student school enrollment | □ |
| | Student grade level | □ |
| | Homeroom | □ |
| | Guidance counselor | □ |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| | Specific curriculum programs | □ |
| | Year of graduation | □ |
| | Other enrollment information- Please specify: | □ |
| Parent/Guardian Contact Information | Address | □ |
| | Email | □ |
| | Phone | □ |
| 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/504) | □ |
| | Living situations (homeless/foster care) | □ |
| | Other indicator information- Please specify: | □ |
| Student Contact Information | Address | □ |
| | Email | □ |
| | Phone | □ |
| Student Identifiers | Local (school district) ID number | □ |

| **Category of Data** | **Elements** | **Check if used by your system** |
|---|---|---|
| | State ID number | □ |
| | Vendor/App assigned student ID number | □ |
| | Student app username | ☑ |
| | Student app passwords | □ |
| | | |
| Student Name | First and/or last | ☑ not required |
| | | |
| 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. | ☑ pupil generated content within their Buncees |

| **Category of Data** | **Elements** | **Check if used by your system** |
|---|---|---|
| | Other student work data – Please specify: | □ |
| | | |
| Transcript | Student course grades | □ |
| | Student course data | □ |
| | Student course grades/performance scores | □ |
| | Other transcript data –Please specify: | □ |
| | | |
| Transportation | Student bus assignment | □ |
| | Student pick-up/drop off location | □ |
| | Student bus card ID | □ |
| | Other transportation data-Please specify: | □ |
| | | |
| Other | Please list each additional data element used, stored or collected through the services as defined in Exhibit A: | □ |
| | | |

# EXHIBIT "B"
# DEFINITIONS

**HB 2087:** The statutory designation for what is now Texas Education Code Texas Education Code Chapter 32 relating to pupil records.

**Data:** Data shall include, but is not limited to, the following: student data, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

**Educational Records:** Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Data.

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Operator removes or obscures any Personally Identifiable Information ("PII") from Data in a way that eliminates the risk of disclosure of the identity of the individual and information about them.

**Data Destruction:** Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.
**NIST 800-63-3:** Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

**Operator:** The term "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 primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. This term shall encompass the term "Third Party," as it is found in applicable state statutes.

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

**Pupil-Generated Content:** The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records.

**Service Agreement:** Refers to the Contract or Purchase Order that this DPA supplements and modifies.
**School Official:** For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Operator's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**Texas Student Privacy Alliance:** The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

**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 pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Operator."

buncee®

# 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 Buncee does the following:

- Complies with federal, state and local data protection laws and follows good practice
- 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

## Our Commitment:

Buncee's commitment to data security and privacy, and more specifically, student privacy is evident throughout our platform. We do not require students to submit email, gender, or DOB. Student accounts created on *Buncee Classroom* or *Buncee for Schools & Districts* are private by default. We do 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 we're a signatory of the Student Privacy Pledge.

Our CEO and COO are both mothers, so as a company, we look at student privacy from the viewpoint of a parent. Our goal is to allow students within Buncee to be able to learn and explore in a safe environment. We implemented our own safe search parameters in order to address CIPA and protect children from harmful online content. Buncee adheres to the data protection rights outlined under GDPR, and is compliant with FERPA and maintaining the confidentiality of student education records. We are also compliant with the Student Online Personal Information Protection Act, aka SOPIPA, as well as the Parent Bill of Rights for Student Data Privacy Act, aka NYSED Law 2-D, and the five criteria the law requires: Purpose, Protection, Disposal, Correction, and Location. As stated above, Buncee participates in the iKeepSafe COPPA Safe Harbor Certification program, and we're a signatory of the Student Privacy Pledge. Protecting students online is our top priority. You can read about our Privacy Policy by accessing this link, https://www.edu.buncee.com/terms-privacy.

## Plan Scope:

This plan applies to the following:

- The officers of Buncee
- All departments of Buncee
- All employees of Buncee
- All contractors and third party operators working on behalf of Buncee

This plan applies to all data** that is submitted to Buncee, more specifically personally identifiable information ("PII"), which may include:

- Names of individuals
- Email addresses
- Dates of birth
- 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 (teacher) of the plan, and is able to create unique usernames/passwords for their students. They are not asked to submit student email or birth data. Under a *Buncee for Schools & Districts* plan, classes, teacher accounts, and student accounts are created by syncing Google Classroom roster data with Buncee, Microsoft Office 365 roster data with Buncee, or by manual upload via CSV file, and do not require the submission of student email or birth data. 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 Buncee 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 Buncee's Privacy Policy and Data Privacy Plan. The manager of each team is responsible for the following:

- Operations/Data Privacy:
  - 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
  - Handling any contracts or agreements pertaining to Buncee's data protection procedures
  - Reviewing current and new data privacy laws and regulations to ensure compliance
- 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

  - Evaluating third-party services to ensure that they are in compliance with Buncee's Privacy Policy and Data Privacy Plan
- Marketing/Sales:
  - Working with Operations and Development to ensure marketing initiatives abide by Buncee's Privacy Policy and Data Privacy Plan
  - Evaluating third-party services to ensure that they are in compliance with Buncee's data collection and protection policies
  - Understanding current and new data privacy laws and regulations to ensure marketing initiatives are in compliance

## Employee Guidelines:

- Only those who need it to perform their duties should have access to data
- Confidential information must be requested from their manager(s)
- Training and guidance will be provided to all employees that will be accessing and handling data (including more specifically, student data)
- Background checks will be performed on all employees with access to data
- When data is stored on paper, employees should follow these guidelines:
  - Keep in a locked drawer when not in use
  - Do not leave papers where others could see them
  - Shred and dispose of paper/printouts when no longer needed
- All data stored electronically should be kept secure by taking the following precautions:
  - Use string passwords that should never be shared
  - Data should never be saved to laptops, mobile devices, or removable media
  - Servers should be protected by security software and a firewall
  - Backup data frequently
  - Never disclose PII to unauthorized people within or outside of Buncee
  - Data should be reviewed, and if no longer required, deleted and disposed of
  - Employees who are uncertain about any aspect of data protection should request guidance from their manager(s)

## Measures to Protect Data:

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 Buncee's engineers
- Publicly accessible parameter for database instances is set to No, thereby disallowing any unauthorized access to the database servers

- SSH key-based authentication is configured on all servers

Buncee serves 100% of its traffic over HTTPS. The HTTPS you see in the URL of your browser means when you go to buncee.com, you're guaranteed to be getting the genuine Buncee website. With HTTPS in place, all interactions with Buncee 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. This applies to all our custom Buncee for Schools & Districts urls too.

Buncee's application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom have rigorous physical measures to safeguard data. 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. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards. 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/) and Security at Digital Ocean (https://www.digitalocean.com/security/).

## Data Storage, Retention, and Access:

User data is stored in secure and managed cloud servers, accessible only to select senior engineers via secure shell. Background checks are performed on all employees who have access to data. User data backups are performed routinely, and securely backed up on the cloud. 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 bcrypt algorithm which is based on the secure blowfish encryption algorithm.

All user data, including, file uploads are stored in the AWS data centers in the following regions: US West (California) and the Digital Ocean data centers in the following regions: US East (New York).

Buncee LLC does not store any user data outside of the United States. However, Buncee 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:

Buncee LLC has implemented the following procedure to manage a data breach:

*Breach Investigation:* Upon discovering a data breach, first and foremost steps are taken to identify the compromised assets and the extent of the breach. A response team consisting of the Product Manager, Director of Engineering and a Senior Software Engineer is created to investigate the breach. Response team will be tasked with isolating the affected systems, including taking the part or the entire site offline.

*Remediation Efforts:* After isolating the damage, review the access logs and the monitoring software to figure out the cause of the breach. Also, consult experts at the cloud hosting service providers to help with the issue. Once the cause is identified, apply and monitor the fix and gradually bring the site online. 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 Product Manager will inform the CEO and COO 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 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 24 hours. Additionally, the response team will monitor the dedicated email address security@buncee.com to address any follow-on questions.

Buncee 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, Buncee 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, teacher, student, or parent.

Under a Buncee Classroom subscription, teacher accounts require the completion of the registration form which requests name, email address, gender, date of birth, name of school, unique username, and password. Student sub-accounts can only be created manually or by class code by the subscriber (teacher) of the *Buncee Classroom* plan, which is able to create unique usernames/passwords for their students, and is not required to submit student email, gender, or birth data. Under a *Buncee for Schools & Districts* subscription, classes, teacher accounts, and student accounts are created by syncing your Google Classroom roster data with Buncee, your Microsoft Office 365 roster data with *Buncee*, by CSV upload, or by manual creation, and do not require the submission of email, gender, or birth data.

Buncee LLC does not sell, rent, or otherwise provide personally identifiable information to any third parties for marketing or advertising purposes.

## Access and Disposal:

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

- What information Buncee 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 Buncee is protecting their data

All requests should be made via email at privacy@buncee.com. The data administrator will then verify the identity of anyone making a request before handing over any information, and will attempt to provide the requestor with the relevant data within 10 business days.

Data for Buncee users is stored for no longer than is necessary to deliver services to the district, school, or individual user, or for school purposes, usually until written notification to terminate the account and delete data has been received from the district, school, or individual user. Buncee will securely delete and/or dispose of any and all data in our possession, including that which was shared with third-party contractors. For specific district procedures when actively cancelling/terminating accounts, if applicable, please refer to your district's Data Sharing Agreement with Buncee for guidelines regarding data deletion.

## Compliance:

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

Buncee is a COPPA Compliant Platform, and Buncee LLC is committed to protecting the privacy of the children who access this platform. Buncee LLC 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). iKeepSafe, which operates one of the seven safe harbor programs approved by FTC has audited and concluded Buncee to be COPPA compliant, after undergoing a rigorous review of Buncee LLC's data security and privacy procedures. Buncee LLC was awarded the iKeepSafe's COPPA badge, making it easy for parents and schools to identify that we are compliant with COPPA.

***Family Educational Rights and Privacy Act (FERPA)**, per http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?*

Buncee is compliant with the Family Educational Rights and Privacy Act (FERPA), and 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. Buncee 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 Buncee 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. Buncee does not sell, rent, or otherwise provide personally identifiable information to any third parties for marketing or advertising purposes. Buncee 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)*** - Buncee 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 website (buncee.com) or mobile application. All searches performed from within the Buncee website (buncee.com) are internally filtered in order to protect children from harmful online content.

***Privacy Act*** - Buncee 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 *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
Buncee 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 Buncee.

***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
Buncee 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 your 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: 20180419_National Data Protection Authorities.pdf.

***NYSED Law 2-D, "The Parent Bill of Rights for Student Data Privacy Act"***, per
https://www.nysenate.gov/legislation/laws/EDN/2-D
Buncee is compliant with NYSED Law 2-D. Buncee does not sell or release a student's personally identifiable information for any commercial purposes, and gives parents the right to inspect and review the complete contents of their child's records. Buncee is in compliance with the five criteria the law requires, as outlined throughout this document, Buncee's Privacy Plan:

- Purpose: the exclusive purpose for which the data will be used

- Protection: how Buncee ensures that contractors, persons or entities that the third party product shared student, principal or teacher data with, if any, will abide by data protection and security requirements employed by Buncee
- Disposal: how student, principal or teacher data is disposed after the expiration of the agreement with the district
- Correction: how a parent, eligible student, teacher or principal may challenge the accuracy of the data that is collected
- Location: where the student, principal or teacher 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