

WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Bellevue School District 405

AGENCY

and

Buncee

06/22/2020

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the Bellevue School District 405 (hereinafter referred to as "LEA") and Buncee (hereinafter referred to as "Provider") on 06/22/2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated 06/22/2020 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family 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 Provider's Services are also subject to several Washington State privacy laws, including Student User Privacy in Education Rights ("SUPER") 28A.604.010 *et seq.*, as well as RCW 19.255.010 *et seq.* and RCW 42.56.590.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records and performing Services pursuant to the Service Agreement; 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 Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Washington 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.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SUPER and other applicable Washington State laws, all as may be amended from time to time. In performing these Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and Services described below and as may be further outlined in Exhibit "A" attached hereto:

Attached

3. **Student 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 "B":

Attached

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C" attached hereto. 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. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer student-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 Student Data in the student's records, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of Services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student Generated Content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said Student Generated Content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Services.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance** LEA shall provide data to Provider for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 CFR § 99.31 (a) (1), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to its computer systems, Services and hosted data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.
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.
3. **Employee Obligation.** Provider shall require all officers, employees and agents (including, but not limited to, Subprocessors) who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure.** De-identified information may be used by the Provider 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). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA, which has provided prior written consent for such transfer. Provider 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. **Disposal of Data.** Upon request, Provider shall dispose of or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposal shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable and/or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposal. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.
 - a. **Partial Disposal During Term of Service Agreement.** Throughout the term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a Student Generated Content account pursuant to Article II, section 3, above. The LEA may also request that specific Student Data be returned to the LEA.

 - b. **Complete Disposal Upon Termination of Service Agreement.** Upon termination of the Service Agreement Provider shall dispose of or delete all Student Data obtained under the Service Agreement. Prior to disposal of the data, Provider shall notify LEA of its option to transfer data to a Student Generated Content account pursuant to Article II, section 3, above, or to other accounts as may be designated by the LEA. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

 - c. **Pre-termination Data Disposal Meeting.** In addition to the foregoing requirements, the LEA may request in writing that Provider participate in a meeting to discuss disposal of the Student Data prior to termination of the Service Agreement.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing,

advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or Services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" attached hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
 - b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposal work authorized under the Service Agreement.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards 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. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital 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.
 - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or who are authorized to access the Provider's computer systems and/or the Student Data. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
 - e. **Mobile Use of Student Data.** Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees, contractors and/or Subprocessors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device

("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device, and a copy of that BYOD policy shall be provided to LEA as part of Exhibit F to this DPA. Provider shall ensure that all contractors and/or Subprocessors implement BYOD policies, which provide for substantially the same level of security for mobile devices as are provided by Provider's BYOD policy.

- f. **Security Technology.** When the Student Data is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
 - g. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
 - h. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically (no less than semi-annually) conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
 - i. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. In the event that the term of the Service Agreement is anticipated to be longer than two (2) years, Provider shall provide written confirmation to the LEA that a third party has conducted a risk assessment analysis of Provider's computer systems at some point during the term of the Service Agreement.
 - j. **Compliance Audit.** LEA shall have the right but shall be under no obligation to conduct audit(s), from time to time, of Provider's records concerning its compliance obligations as set forth in this Article V. Provider shall make such records and other documents available to LEA upon request.
2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA immediately following discovery of the incident. Provider shall follow the following process:
- a. 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.

- b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting Provider subject to this section.
 - ii. A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation and the law enforcement agency determined that notification would impede a criminal investigation.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. Information about what the Provider has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

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

- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

- f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

- g. In the event of a breach originating from LEA's use of the Service, Provider shall

cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI – INDEMNITY

I. Indemnity. Provider shall defend, indemnify and hold harmless the LEA, its officers, directors, employees, agents and assigns (the “Indemnitees”) from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys’ fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance carrier, arising out of or resulting from any third-party claim against the Indemnitees arising out of or resulting from Provider’s failure to comply with any of its obligations under this DPA. Provider’s duty to defend and indemnify the LEA includes any and all claims and causes of action whether based in tort, contract, statute, or equity. Provider agrees that it shall be obligated to accept any tender of defense by the LEA pursuant to this DPA and provide a full defense to the LEA so long as any potential exists for Provider to have an obligation to indemnify the LEA for any part of any potential judgment against the LEA.

Provider’s defense and indemnity obligations herein are intended to provide for the broadest indemnity rights available under Washington law and shall survive the termination of this DPA. To the extent Provider’s defense and indemnity obligations as set forth in this DPA conflict with the terms of the Service Agreement, the defense and indemnity provisions set forth herein shall control.

ARTICLE VII- GENERAL OFFER OF PRIVACY TERMS

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

ARTICLE VIII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for a period of three (3) years, or so long as the Provider performs services under this Agreement, whichever shall be longer.
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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach by Provider, its employees, or agents of the terms of this DPA.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA’s data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. No indemnification provisions granted by

the LEA in the Service Agreement shall be effective as to a breach of the terms of this DPA by the Provider. 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 e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this DPA is:

Name: James Luke
Title: Director of Cyber Security

Contact Information:
lukej@bsd405.org
12241 Main Street, Bldg 6
Bellevue, WA 98005

The designated representative for the Provider for this DPA is:

Name: Claire Cucchi
Title: Chief Operations Officer

Contact Information:
170 Montauk Highwaym Speonk NY 11972
(631) 591-1390
claire@buncee.com

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Claire Cucchi
Title: Chief Operations Officer


Contact Information:
170 Montauk Highwaym Speonk NY 11972
(631) 591-1390
claire@buncee.com

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 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 WASHINGTON, 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 THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Successors Bound**. This DPA is and shall be binding upon Provider's respective successors in interest in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

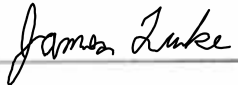
[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Washington Student Data Privacy Agreement as of the last day noted below.

Name of Provider Buncee
BY:  Date: 06/22/2020

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

Address for Notice Purposes:

Name of Local Education Agency Bellevue School District 405
BY:  Date: 06/22/2020

Printed Name: James Luke Title/Position: Director of Cyber Security

Address for Notice Purposes:

12241 Main Street, Bldg 6, Bellevue, WA 98005

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

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, across grade, age and learning levels. Buncee is a one-stop-shop to build media-rich lessons, reports, newsletters, presentations and so much more!

Buncee's web-based creation and communication tool, *Buncee V.3*, enables classrooms and administrators to create, publish, and distribute original and authentic content. 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 a classroom dashboard, access to a template library, 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 Educational Resource Library, the ability to customize your organization's own templates and graphics library; and an administrative management dashboard to monitor user permissions and privacy and synchronize rosters.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	x
	Other application technology meta data-Please specify:	X Browser agent
Application Use Statistics	Meta data on user interaction with application	X 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 communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	

Category of Data	Elements	Check if used by your system
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
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	

Category of Data	Elements	Check if used by your system
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	x
	Student app passwords	
Student Name	First and/or Last	X Not required
Student In App Performance	Program/application performance (tutoring program)	

Category of Data	Elements	Check if used by your system
	wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	X Within their Buncee creations
	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 and/or drop off location	
	Student bus card ID number	
	Other transportation	

Category of Data	Elements	Check if used by your system
	specify:	
Other	Please list each additional data element used, stored or collected by your application	

No Student Data Collected at this time _____.

*Provider shall immediately notify LEA if this designation is no longer applicable.

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the States of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

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 as identified by Washington Compact Provision 28A.705.010. The categories of Educational Records under Washington law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

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

Indirect Identifiers: Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator (*e.g.*, state, county) and other descriptors.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication 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. For the purpose of the Data Privacy Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Persistent Unique Identifiers. A long-lasting identification for digital objects, which allows for those digital objects to be located even if they are moved or removed.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or student-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider 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 Student Data.

Provider: For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or Services, including cloud-based services, for the digital storage, management, and retrieval of student records. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

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, and Student Personal Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which 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.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identities, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of federal laws and regulations. Student Data as specified in Exhibit “B” is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s Services.

Student Generated Content: The term “Student Generated Content” means materials or content created by a student 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 student content.

Student Personal Information: “Student Personal Information” means information collected through a school service that personally identifies an individual student or other information

collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

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

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 Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 student 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 "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSAL OF DATA

Bellevue School District 405 (hereinafter referred to as "LEA") directs [Buncee
(hereinafter referred to as "Provider") to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. Unless modified by separate agreement pursuant to a pre-termination data disposal meeting as described in Article IV Section 5(c), the terms of the Disposal are set forth below:

<u>Extent of Disposal</u>	Disposal shall be:	<input type="checkbox"/> Partial. The categories of data to be disposed of are set forth in an attachment to this Directive. <input type="checkbox"/> Complete. Disposal extends to all categories of data.
<u>Nature of Disposal</u>	Disposal shall be by:	<input type="checkbox"/> Destruction or deletion of data. <input type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
<u>Timing of Disposal</u>	Data shall be disposed of by the following date:	<input type="checkbox"/> As soon as commercially practicable <input type="checkbox"/> By (Insert Date) _____ Insert or attach special instructions

Authorized Representative of LEA

Date

Verification of Disposal of Data
by Authorized Representative of Provider

Date

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Please see attached Data Privacy Plan



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 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
- When data is stored on paper, employees 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 is kept secure by taking the following precautions:
 - Use string passwords that should never be shared
 - Data is never be saved to laptops, mobile devices, or removable media
 - Servers are protected by security software and a firewall
 - Backup data frequently
 - Never disclose PII to unauthorized people within or outside of Buncee
 - Data is reviewed, and if no longer required, deleted and disposed of
 - Routinely monitor systems for security breaches and attempts of inappropriate access
 - 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 uses SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees) is encrypted at rest. All passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm.

Account information is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers. 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.

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, and are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. 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 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: [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, 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 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

For more information about Buncee's commitment to protecting you and your data online, please refer to our Privacy Policy at <https://app.edu.buncee.com/terms-privacy#privacy>.