



STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0/ with Exhibit E)

Mesa Unified School District #4

and

[Blooket LLC]

Version: 1r6

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between:

Mesa Unified School District, located at 63 E Main St, Mesa Az, 85201 (the “Local Education Agency” or “LEA”) and
Blooket LLC

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

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Nathan Myers Title: Educational Technology Director

Address: 549 N Stapley Drive, Mesa Az, 85203

Phone: 480-472-0012 Email: namyers@mpsaz.org

The designated representative for the Provider for this DPA is:

Name: Gregory D. Stewart Title: Managing Member

Address: 409 South Ridge Ave. Middletown DE 19709

Phone: (302) 828-0101 Email: gstewart@gregstewartlaw.com


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

LEA Mesa Unified School District

By:  Date: 11/08/2021

Printed Name: Nathan Myers Title/Position: Educational Technology Director

Blooket LLC

By:  Date: 10/18/2021

Printed Name: Gregory D. Stewart Title/Position: Managing Member

STANDARD CLAUSES

Version 1.0

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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 LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

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

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between

Exhibit "H", the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

The educational website Blooket.com.

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.	xx
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	

Category of Data	Elements	Check if Used by Your System
	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	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	XX
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	XX
	Student app passwords	XX
Student Name	First and/or Last	XX
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.	

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 and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"**DEFINITIONS**

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

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

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

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

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

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

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

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

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

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Mesa Unified School District #4 directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [_____]Date

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Mesa Unified School District ("Originating LEA") which is dated [10/18/21 Date], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: gstewart@gregstewartlaw.com

Blooket LLC

BY:  Date: 10/18/2021

Printed Name: Gregory D. Stewart Title/Position: Managing Member

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Mesa Unified School District and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

[_____ Subscribing LEA]

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____ Title: _____

Address: _____

Telephone Number: _____ Email: _____

EXHIBIT " F "

DATA SECURITY

1. **Operator's Security Contact Information:**

Gregory D. Stewart [Box 26]

Named Security Contact

gstewart@gregstewartlaw.com [Box 27]

Email of Security Contact

(302) 828-0101 [Box 28]

Phone Number of Security Contact

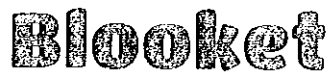
2. **List of Operator's Subprocessors:**

The list is located at <https://www.blooket.com/privacy>. [Box 29]

3. **Additional Data Security Measures:**

[Box 30]

Data encryption, password protection and firewalls.



Blooket Privacy Policy

Last updated January 25, 2021

Blooket LLC operates Blooket.com. We would first like to thank the users and educators who have made this website possible. The privacy of our users is very important to us.

Blooket LLC ("BLOOKET") is concerned about the protection of privacy of all of our users. Blooket wants you to be familiar with how we collect, use and disclose information. This Privacy Policy describes our practices in connection with information that we collect through websites operated by us from which you are accessing this Privacy Policy (the "Website") and through HTML-formatted email messages that we send that link to this Privacy Policy (collectively, the "Services"). By providing Personal Information to us, you agree to the terms and conditions of this Privacy Policy.

**BLOOKET IS COMMITTED TO REMAINING AN AD FREE SERVICE TO OUR USERS.
BLOOKET WILL NOT ADVERTISE IN ANY FORM ON THE SITE.**

This Privacy Policy explains:

- What information Blooket collects from you (and why we collect it).
- How we use and share that information.
- The choices you have, including how to access, update and delete your information.
- This Policy applies to all services offered by Blooket LLC (hereinafter referred to as "Blooket," "we," "us," and "our,").
- This policy applies to Blooket Users and Visitors as well as educators and schools who utilize the service in a classroom setting. Blooket users are our registered account holders. Blooket Visitors are parties invited to play a game or engage in homework by a registered user or school. The only information collected from visitors is a username of their choice.

We have done our best to write this Policy in simple, clear terms. We encourage you to read it carefully, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

- Purpose of processing: provide access to and use of Blooket.com.
- Legal grounds: processing based on user consent, contract performance and the legitimate interest of the company or third parties.
- Recipients: Blooket third-party service providers which help provide the Service. Please see the Security measures section of this Privacy Policy for more information.

- User rights: access, rectification, erasure, restriction, objection and data portability (see the Blooket Privacy Principles section of this Privacy Policy).
- Inquiries: for inquiries regarding this Privacy Policy please contact Blooket at contact-us@blooket.com or at the physical address listed at the end of this Policy.
- Additional information: to be found in Blooket's Terms of Service and this Privacy Policy.

Personal information is any information you provide to us that personally identifies you, like your name or email address, or any other information which we could reasonably link to your identity. We will only collect, use, and share your personal information in accordance with this Privacy Policy. This Policy applies whether you use Blooket through [Blooket.com](https://www.blooket.com). In addition, this Privacy Policy also covers Blooket's treatment of any personal information about our users that our partners or other services might share with us. This Policy does not apply to websites or services or practices of companies that Blooket does not own or control. These other services have their own privacy policies, and we encourage you to review them before providing them with personal information. At the end of this Privacy Policy you will find a list with our third-party service providers and a link to their privacy policies, as well as an overview to how, why and under which conditions they might process your personal information. Whether you are new here (welcome!), or have been using Blooket for a long time (welcome back!), please do take the time to get to know our privacy practices. We believe them to be fairly clear and friendly, but if you have any questions, we are here to help. To learn more about how we protect your privacy, send us an email at contact-us@blooket.com. BY USING THE SERVICE, YOU ACKNOWLEDGE THAT YOU ACCEPT AND AGREE TO THIS PRIVACY POLICY. This Privacy Policy applies to your use of the Blooket Services and personal data transferred to third countries which do not ensure an adequate level of data protection. In addition to the foregoing, and to further secure transfers of personal data to the United States, Blooket also complies with the EU-US and Swiss-US Privacy Shield Frameworks as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries, the United Kingdom and Switzerland, respectively. Blooket remains responsible for any of your personal information that is shared under the Onward Transfer Principle with third parties for external processing on your behalf, as described in the Europe section of this Privacy Policy.

Blooket

Blooket provides a game-based learning tool that can be played through most web browsers (<https://www.blooket.com>). Blooket is an exciting new take on trivia and review games! Blooket creates an engaged learning environment that motivates students. One player or teacher hosts the game, and everyone else competes on their own devices.

Blooket Privacy Principles

In collecting and processing your personal information, we will comply with the data protection laws and regulations in force at the time. This requires that the personal

information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in a way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up-to-date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Collection of Personal Information

Blooket collects personal information from users in order to provide the Service. Concretely, the personal information of students and teachers is collected and used for the following purposes:

- To create the necessary accounts to use the Service.
- To assess the quality of the Service.
- To secure and safeguard personal information.
- To access premium features, if applicable.
- To comply with all applicable laws on the protection of personal information.

Rights Regarding Personal Information

Your rights relating to your personal information include:

- to be informed about how Blooket uses your personal information;
- to request access to personal information held by Blooket, and to have any incorrect, inaccurate or incomplete personal information rectified;
- where appropriate, to restrict processing concerning you or to object to processing;
- to have personal information erased where there is no compelling reason for its continued processing; and
- where applicable, to portability of personal data, that is to say, to receive your personal information in a structured and commonly used format.

Responsibilities of Users of Blooket.com

We require that your personal information is accurate. Please let us know if the personal information you provided us for creating your account has changed. If we do not have the correct information, we cannot take responsibility for information-related errors. Additionally, if we determine that you are in violation of this Policy, you will be subject to disciplinary action that could eventually lead to the banning of your account.

Transparency and Choice

We try to be transparent about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Access and manage your account information by using the account settings within Blooket.
- Delete your account and information.

Notice

When providing you with information on the processing of your personal information, such as its collection, transfer to other countries, types or identity of third parties to which we disclose that information and the purposes for which we do so, we will make sure that such information is provided in clear and understandable language. Also, initial notice on our practices and policies will be provided when you are first asked to provide personal information to us, or as soon as practicable thereafter, and in any event before we use the information for a purpose other than that for which it was originally collected.

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason which is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Contract Performance

When you create a Blooket account, you provide your first and last name and an email address. We require those data elements for you to enter into the Terms of Service agreement with us, and we process those elements on the basis of performing that contract.

Consent

Please note that Blooket provides its Service upon explicit consent given by you when signing up. Prior to signing up, we will direct you to our Terms of Use and this Privacy Policy. When signing up, you will be declaring to have read such policies and to consent to them. Remember, nonetheless, that you will be able to withdraw your consent at any time by deleting your account by contacting Blooket to have your account deleted. EDUCATIONAL INSTITUTIONS AND EDUCATORS UTILIZING THE SERVICE ARE RESPONSIBLE FOR MONITORING THE RIGHTS AND INTERESTS OF THEIR STUDENTS AND MUST THEREFORE TAKE SPECIAL CARE WHEN REVIEWING THIS PRIVACY POLICY. EDUCATIONAL INSTITUTIONS AND EDUCATORS SHALL BE RESPONSIBLE FOR OBTAINING, WHERE APPLICABLE, PERTINENT CONSENT FROM PARENTS, LEGAL GUARDIANS OR ELIGIBLE STUDENTS (THOSE WHO ARE 18 YEARS OF AGE OR ATTEND A POSTSECONDARY INSTITUTION) PRIOR TO UTILIZING THE SERVICE. BLOOKET SHALL NOT BE RESPONSIBLE FOR ANY NEGLIGENCE OF THE EDUCATIONAL INSTITUTION IN THE REVIEWING OF THIS PRIVACY POLICY OR THE OBTAINMENT, WHERE APPLICABLE,

OF THE NECESSARY PARENTAL CONSENT. U.S. Educational Institutions and Parental Consent: Consistent with the requirements of COPPA, if you or your school decide to utilize the Service with children under 13, you will be electing to either obtain parental consent or to consent on behalf of the children's parents directly, which is commonly referred to as "school consent." At the same time, yet subject to exceptions, FERPA prohibits schools from disclosing personally identifiable information from a student's education record to a third party without written consent from the parent or eligible student. Accordingly, schools must either obtain parental consent, or ensure that their use of BlooKet meets one of FERPA's exceptions to the written consent requirement. Typically, schools are exempted from obtaining parental consent under FERPA when BlooKet is identified as a "school official," meaning BlooKet is performing an institutional service or function for which the school would otherwise use its own employees. Educators and schools may disclose certain information about students under the exception to FERPA's general prior consent rule that are set forth in the statute and the regulations for the disclosure of "directory information" if the school follows certain procedures set forth in FERPA. (34 CFR § 99.31(a)(11).) FERPA defines "directory information" as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." The means of notification could include publication in various sources, including a newsletter, in a local newspaper, or in the student handbook. The school could also include the "directory information" notification as part of the general notification of rights under FERPA. The school does not have to notify a parent or eligible student individually.

European Educational Institutions and GDPR: According to article 8 of the GDPR, minors shall be entitled to give valid consent only if they are 16 years old (unless Member States have set a lower age limit which, nonetheless, cannot be under 13 years old). Under that age limit, processing of personal information related to minors shall be subject to parental consent. Schools are in control of their students' personal information and are obliged to take all necessary measures for protecting said information. This means that schools will have to be especially cautious when contracting any service that may require disclosure of student personal information. In other words, schools are data controllers in terms of GDPR and thus determine the purposes and means of the processing of student personal data. As a consequence, schools will also be responsible for informing students and their parents accordingly about what data is collected, which are the purposes of collection, how data is used and to which third parties it is disclosed, including BlooKet.

Legitimate Interests

Generally, the remainder of the processing of personal information we perform is necessary for the purposes of our legitimate interests or those of third parties. For example, for legal compliance purposes or to maintain ongoing confidentiality, integrity, availability and resilience of Blooket's systems, website, and overall services, we must keep logs of Technical Information. As foreseen in the "Restrictions" and "Account Bans" sections of our Terms of Service, the breach of certain rules in the use of the Service may lead to the suspension or indefinite ban of your account, depending on the severity of the offense. In the event of an indefinite account ban, Blooket may keep part of your personal information, such as, but not limited to, IP address and email address, to prevent you from accessing or using the Service.

Notice of Changes of Policy

We may occasionally update this Privacy Policy. You can see when the last update was by looking at the "Last Updated" date at the top of this page. We will not reduce your rights under this Privacy Policy without your explicit consent. If we make any significant changes, we will provide prominent notice by posting a notice on the Service and/or notifying you by email (using the email address you provided) prior to and after changes taking effect, so you can review and make sure you're aware of them. We encourage you to review this Privacy Policy from time to time, to stay informed about our collection, use, and disclosure of personal information through the Service. If you do not agree with any changes to the Privacy Policy, you may delete your account (although we will be sad to see you go!). By continuing to use the Service after the revised Privacy Policy has become effective, you acknowledge that you accept and agree to the current version of the Privacy Policy.

Protecting the Privacy Rights of Children

Blooket permits registered users to invite visitors to the website. Visitors are only required to provide a username to play a game or complete a homework assignment. Blooket permits children under the age of thirteen to become users only with parental consent.

Blooket collects the minimal amount of information from users necessary to create accounts on our Service. Beyond this information, users and visitors can submit responses. In addition to the information entered by the child, we automatically collect some information from any use of our Service as set forth in the "Information Collected Automatically" section. We use this information to provide the Service to the child, for security and safety purposes, or as required by law or to enforce our Terms. We will not require children to provide more personal information than is reasonably necessary in order to participate in the Service. If we discover that we have collected information from a child in a manner inconsistent with COPPA, FERPA or any other applicable laws or regulations, we will take appropriate steps to delete the information. We do not disclose any personal information about children to third parties, except to service providers necessary to provide the Service, as required by law, or to protect the security of the Service or other users. Information collected from students (including personal information and information collected automatically) is never used or disclosed for third-party advertising, including any kind of first- or third-party behaviorally

targeted advertising, and children's personal information is never sold or rented to anyone, including marketers or advertisers.

Blooket does not permit children under the age of 13 (a "Child" or "Children") to create an account without the consent and at the direction of a Parent or School official consenting in loco parentis. Children under 13 may create an account with the parent's consent.

When Blooket is used by a School in an educational setting, we may rely on the School to provide the requisite consent for Blooket to collect information from a School User under the age of 13, in lieu of parental consent.

Information regarding Children

No student's profile is made available or visible to the public, or to any other students, through Blooket. If the teacher chooses to display Blooket in their classroom by projecting via a smartboard or interactive whiteboard, students physically present in that classroom may see other students' usernames, responses, comments or total scores. EDUCATIONAL INSTITUTIONS AND TEACHERS SHALL MAKE A RESPONSIBLE USE OF THE SERVICE AND AVOID COMPROMISING CHILDREN'S PERSONAL INFORMATION AT ALL TIMES WHEN DISPLAYING BLOOKET IN THE CLASSROOM. BLOOKET SHALL NOT BE HELD LIABLE FOR THE INAPPROPRIATE USE OF THE SERVICE BY THE EDUCATIONAL INSTITUTION OR THE TEACHER.

Storage of Data

We store the data of visitors including usernames in order to allow users to evaluate the homework or evaluate participation in games.

- **Minimal information:** As mentioned before, Blooket collects the minimal amount of information from students necessary to utilize our Service: we ask student who are invited to play the games or participate in homework to only create a username. Students who join as users with parental consent or who are above specified ages only provide names, email addresses and usernames. Consistent with the requirements of FERPA and COPPA in the United States and of GDPR in Europe, among other applicable laws, we only collect, use, share, and retain student personal information for purposes for which we were authorized by the educational institution/agency, teacher or the student. Beyond this information, students can submit responses depending on the activities they are assigned, that will remain private between teacher and student. In addition to the information entered by the child, we automatically collect some information from any use of our Service as set forth in the "Information collected automatically" section.
- **Deleting inactive accounts:** Blooket will delete inactive accounts and data in compliance with the data retention policy of the company.

After deletion of the account or data, Blooket may retain copies and/or backups of the mentioned information for a maximum term of eighteen (18) months. Nevertheless, Blooket shall not be responsible for the accidental loss or destruction of data on behalf of users. Blooket will not be obliged to recover erased data stored in backups when erasure is

attributable to users. EDUCATIONAL INSTITUTIONS UTILIZING THE SERVICE ARE RESPONSIBLE FOR COMPLYING WITH THE RETENTION OF STUDENT EDUCATION RECORDS FOR AS LONG AS LEGALLY APPLICABLE. STUDENT PROGRESS MAY BE SAVED FOR EITHER SHORTER OR LONGER PERIODS THAN THE ONES STATED ABOVE IF SO DECIDED BY THE EDUCATIONAL INSTITUTION. TEACHER ACCOUNTS WILL BE PROVIDED WITH NECESSARY TOOLS TO MANAGE AND DELETE STUDENT INFORMATION. BLOOKET SHALL NOT BE RESPONSIBLE FOR ERASURE OF STUDENT PROGRESS DUE TO ACCOUNT DELETION AFTER AN EXTENDED PERIOD OF INACTIVITY OR BECAUSE OF THE VOLUNTARY ELECTION TO DELETE TEACHER ACCOUNTS. SCHOOL OFFICIALS MAY REQUEST DELETION OF STUDENT INFORMATION AND CONTENT AT ANY TIME BY CONTACTING BLOOKET AT CONTACT-US@BLOOKET.COM.

Parental Choices

Any parents that want copies of their children's personal information that we may have stored can contact their children's school personnel to that end. If a parent has authorized an account, they also may contact Blooket to retrieve their child's personal information. At any time, the school can also refuse to permit us to collect further personal information from its students, and can request that we delete the personal information we have collected from them by contacting us at contact-us@Blooket.com. Please keep in mind that deleting records may require us to terminate the account in question. Also remember that before we can share the information with the school, or delete it per your request, we will, by reasonable means, proceed to verify the identity of the requester.

Information Collected

Blooket collects two types of information about you: (1) information that you voluntarily provide us by using the Blooket Service (described below under "Information you provide to us") and (2) information collected automatically as result of your use of the Service (described below under "Information collected automatically"). The types and amounts of information collected will vary depending on whether the user is a visitor to the site invited to participate in a game. Only minimal information is collected for both users and visitors

Information You Provide to Us

There are currently two categories of users on our Service: users and visitors. We collect and store the following types of information from each type of user:

- **Account Sign-up and Profile Information:** To create a Blooket account, you may be asked to provide some basic information. If you create an Blooket account as a user, you will be asked to enter your first name, last name, username, password and email. Visitors who participate in games will be asked only for a username.
- **Contact Information:** When you choose to provide us with your personal information through the Service in some other manner (e.g., when you request a quote for upgrading to a "Blooket Plus", when you submit a copyright claim or report any media

on our platform, when you send us an email asking a question, or submit a support request).

- **Billing Information:** When subscribing to any of our "Blooket Plus" options, you will be asked to provide necessary information for processing the payment (e.g., credit/debit card number). As further explained in the Security Measures section of this Privacy Policy, payments are processed over Stripe through their third party website service.

Information Collected Automatically

Like most web-based services, we (or our service providers) may automatically receive and log information on our server logs from your browser or your device when you use the Service. For example, this could include the frequency and duration of your visits to Blooket. If you use Blooket on different devices, we may link the information we collect from those different devices to help us provide a consistent Service across your different devices. If we do combine any automatically-collected information with personal information, we will treat the combined information as personal information, and it will be protected as per this Privacy Policy. The technologies and information we automatically collect include:

- **Cookies and Other Similar Technologies:** We (or our service providers) may use various technologies to collect and store information when you visit our Service, including clear GIFs (also known as "web beacons"), "tags", "scripts", and "cookies". We also make use of persistent secure cookies: persistent cookie remains after you close your browser (although they can be removed) and may be used by your browser to identify you on subsequent visits to the Service. We may also use, collect and store information locally on your device using mechanisms such as browser web storage (including HTML 5). Like many services, Blooket uses these technologies to tailor the Service for you, and to help the Service work better for you - for example, by remembering your language preferences.
- **Device Information:** We collect, through our third-party analytics services, device-specific information such as your operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers. This helps us measure how the Service is performing, improve Blooket for you on your particular device, and send you push notifications if you've opted in to receive them.
- **Log Information:** Like most online services, when you use our Service, we automatically collect and store certain information in our server logs. Examples include:
 - Details of how you used our service, such as your activity on the Service, and the frequency and duration of your visits to the Blooket Website.
 - IP Address.
 - Device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.

This information helps us make decisions about what we should work on next - for example, by showing which features are most (or least!) popular.

- **Location Information:** When you use our Service we may collect and process information about your geographic location, for example through GPS, Bluetooth, or Wi-Fi signals. We collect coarse (i.e., city-level) location data. We will not store or track your device location on an ongoing basis or without your permission. We do not share precise geolocation data with third parties, other than our service providers as necessary to provide the Service.

Automated Decision Making and Profiling

Automated Decision Making (ADM) refers to a decision which is taken solely on the basis of automated processing of your personal data. This means processing using, for example, software code or an algorithm, which does not require human intervention. Profiling means using automated processes without human intervention (such as computer programs) to analyze your personal information in order to evaluate your behavior or to predict things about you which are relevant in the context of using Blooket, such as what kind of games or Blooket sets you utilized. As profiling uses automated processing, it is sometimes connected with automated decision-making. Not all profiling results in automated decision-making, but it can.

Use of Information by Blooket

First and foremost, you should know that Blooket does not sell or rent any personal information to any third party for any purpose including for advertising or marketing purposes. We use the information we collect from you to provide you with the best Blooket experience. More specifically, this information is used to:

- Provide and improve the Service, for example by developing new products and features.
- Respond to your requests for information or customer support.
- Customize the Service for you, and improve your experience with it.
- Send you information about new features and Blooket products we believe you may be interested in.
- Most crucially, to protect our community by making sure the Service remains safe and secure.

We use automatically collected information (described in the "Information Collected Automatically" section above) to provide and support our Service, and for the additional uses described in this section of our Privacy Policy.

Storage of Data

We store your personal information for as long as it is necessary to provide products and Services to you and others, including those described above pursuant to our Data Retention Policy. Deletion will affect any on-going paid subscriptions, which will be immediately cancelled. Note we may retain and use de-identified data (i.e., data which has been stripped

off all information that can be used to identify a person) for purposes of research, improvement of our products and services, and/or the development of new products and services. We may also have to retain some information after your account is deleted, to comply with legal obligations, to protect the safety and security of our community or our Service, or to prevent abuse of our Terms. In case we keep copies or backups of personal information, such copies or backups will be kept for a maximum term of eighteen (18) months after the deletion of your account.

Security Measures

First and foremost, you should know that Blooket does not sell or rent your, or your students' personal information to any third party for any purpose - including for advertising or marketing purposes. Furthermore, we do not share personal information with any third parties except in the limited circumstances described in this Privacy Policy. No student profiles are made available to the general public through our Service. Furthermore, students cannot share their account information with anyone on Blooket. If you are a user, you may choose to share information or content through the Service with other Blooket users - for example, things like your account information or Blooket sets. Please keep in mind that information (including personal information or children's personal information) or content that you voluntarily disclose to others - including other Blooket users you interact with through the Service can be viewed, copied, stored, and used by the people you share it with. We cannot control the actions of people with whom you choose to share information.

- **Service Providers:** We do work with vendors, service providers, and other partners to help us provide the Service by performing tasks on our behalf - we can't build everything ourselves, after all! We may need to share or provide information (including personal information) to them to help them perform these business functions, for example sending emails on our behalf, database management services, database hosting, providing customer support software, and security. Generally, these service providers do not have the right to use your personal information we share with them beyond what is necessary to assist us. Additionally, these service providers must adhere to confidentiality and security obligations in a way that is consistent with this Privacy Policy.
- **Analytics Services:** We use analytics services, including mobile analytics software, to help us understand and improve how the Service is being used. These services may collect, store and use information in order to help us understand things like how often you use the Service, the events that occur within the application, usage, performance data, and from where the application was downloaded.
- **Aggregated Information and Non-Identifying Information:** We may share aggregated, non-personally identifiable information publicly, including with users, partners or the press in order to, for example, demonstrate how Blooket is used, spot industry trends, or to provide marketing materials for Blooket. Any aggregated information shared this way will not contain any personal information.

- **Legal Requirements:** We may disclose personal information if we have a good faith belief that doing so is necessary to comply with the law, such as complying with a subpoena or other legal process. We may need to disclose personal information where, in good faith, we think it is necessary to protect the rights, property, or safety of Blooket, our employees, our community, or others, or to prevent violations of our Terms of Service or other agreements. This includes, without limitation, exchanging information with other companies and organizations for fraud protection or responding to government requests.
- **Sharing with Blooket Companies:** Over time, Blooket may grow and reorganize. We may share your personal information with affiliates such as a parent company, subsidiaries, joint venture partners or other companies that we control or that are under common control by us, in which case we will require those companies to agree to use your personal information in a way that is consistent with this Privacy Policy.
- **Change of Control:** In the event that all or a portion of Blooket or its assets are acquired by or merged with a third party, personal information that we have collected from users would be one of the assets transferred to or acquired by that third party. This Privacy Policy will continue to apply to your information, and any acquirer would only be able to handle your personal information as per this policy (unless you give consent to a new policy). We will provide you with notice of an acquisition within thirty (30) days following the completion of such a transaction, by posting on our homepage, and by email to your email address that you provided to us. If you do not consent to the use of your personal information by such a successor company, you may request its deletion from the company. In the unlikely event that Blooket goes out of business, or files for bankruptcy, we will protect your personal information, and will not sell it to any third party.
- **With your Consent:** Other than the cases above, we won't disclose your personal information for any purpose unless you consent to it. Additionally, as discussed above, we will never sell or rent your personal information to advertisers or other third parties.

Do Not Track

Blooket does not track its users over time and across third-party websites to provide targeted advertising and therefore does not respond to Do Not Track (DNT) signals.

Blooket's Third-Party Service Providers

It is important to us that we keep your information safe and secure. To best provide our services, and keep your information safe, we work with a few other companies (we can't do it all ourselves!). These companies ("third-party service providers", "collaborators" or "agents") will only have access to the information they need to provide the Blooket service. Below is a list of the service providers which, subject to their terms of service and privacy policies, may have access to personal data to process on our behalf in accordance with our instructions, Privacy Policy and any other requirements regarding confidentiality, security or integrity:

- Google Services for analytics on our website ("Google Analytics"), for mobile analytics ("Fabric") and for spam and abuse protection ("reCAPTCHA").
- Cloundinary for creating, managing and delivering digital images and media across any browser.
- SendGrid to manage and automate email communications.
- MongoDB is a general purpose, document-based, distributed database built for modern application developers and for the cloud era.
- Heroku is a platform used to host the main website servers.
- Stripe as a payment processing service.

This list may change over time, and we will work hard to keep it up-to-date. Blooket reserves the right to change or add service providers which provide services in concert with the provisions of this agreement.

Accountability for Onward Transfer

We will transfer your personal information to third-party service providers only for limited and specific purposes. We will obtain contractual assurances from our collaborators that they will safeguard personal information in a manner consistent with this Policy and that they will provide the same level of protection as per best industry standards. We recognize our responsibility and potential liability for onward transfers to agents. Where we have knowledge that an agent is using or disclosing personal information in a manner contrary to this Policy and/or level of protection as required by applicable laws and regulations, we will take reasonable steps to prevent, remediate or stop such use or disclosure. If we transfer personal information to non-agent third parties, that is to say, any new collaborators that are not included in the previously mentioned list, we will (1) notify you with all necessary information on any key elements affecting the processing of your personal data, and (2) obtain contractual assurance from these parties that they will provide the same level of security as per best industry standards and in accordance with any applicable laws and regulations.

Blooket Account Security

Your Blooket account is protected by a password. You can help us protect your account from unauthorized access by keeping your password secret at all times. The security of your personal information is important to us. We work hard to protect our community, and we maintain administrative, technical and physical safeguards designed to protect against unauthorized use, disclosure of or access to personal information, such as:

- Security Protocols: We periodically review our information collection, storage and processing practices, including physical security measures, to protect against unauthorized access to systems.
- Security Technology: We continually develop and implement features to keep your personal information safe - for example, when you enter any information anywhere on

the Service, we encrypt the transmission of that information using secure socket layer technology (SSL) by default.

- We ensure passwords are stored and transferred securely using encryption and hashing.
- Employee Access: We use best-effort practices to secure usernames, passwords and any other means of gaining access to users' data.

Notification of Security Breaches

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems as per best industry standards, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time.

- Initial Notice: Upon the discovery of a security breach that results in the unauthorized release, disclosure or acquisition of personal information, we will notify electronically of such discovery to all affected users. This initial notice will include, to the extent known at the time of the notification, the date and time of the breach, its nature and extent, and the Service's plan to investigate and remediate the breach.
- Detailed Notification: Upon discovery of a breach, we will conduct a deep investigation in order to electronically provide all affected users with a more detailed notice of the breach, including but not limited to the date and time of the breach; nature and extent of the breach; and measures taken to ensure that such breach does not occur in the future. We may also post a notice on our homepage (www.Blooket.com) and, depending on where you live, you may have a legal right to receive notice of a security breach in writing. When it is not possible to provide all of the aforementioned information at the same time, we will provide you with the remaining information without undue further delay.

Both notifications will be written in plain language, will be titled "Notice of Data Breach" and will present the information described above under the following heading: "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.

Managing My Information

Upon request and in accordance with the applicable laws and regulations, we will grant you reasonable access to your personal information that is held by Blooket. In addition, we will take reasonable steps to permit you to correct, amend, or delete your personal information that is demonstrated to be inaccurate, incomplete or processed in violation of this Privacy Policy.

- **Accessing Your Information:** To request access to the personal information we have about you on file, users can contact us at contact-us@Blooket.com. In some cases, we will not be able to guarantee complete access due to legal restrictions; for example, you will not be allowed to access files that contain information about other users or information that is confidential to us. Furthermore, we may not be able to fulfill requests that are unreasonably repetitive, require disproportionate technical effort or would be extremely impractical.
- **Updating Your Information:** You may update, correct, or delete some of your profile information or your preferences at any time by logging into your account on Blooket and accessing your account settings page. You may also, at any time, update, correct, or delete certain personal information that you have provided to us. To that end, users can contact us at contact-us@Blooket.com. Please note that while your changes may be reflected promptly in active content, users that have previously accessed the content may still have access to old copies cached on their device or may have copied and stored your content. In addition, we may retain a backup copy of the prior version for a limited period of time (maximum 18 months) or for legal purposes.
- **Limitations:** Without prejudice to the aforementioned, please note that we may limit or deny access to personal information (a) where the burden or expense of providing access would be disproportionate to the risks to your privacy; (b) where the legitimate rights of persons other than you would be violated or if necessary to safeguard important countervailing public interests (e.g., national security) or in other limited circumstances (e.g., disclosure would breach a legal privilege), and (c) where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal information that we hold about you. In addition, the personal information may have been destroyed, erased or made anonymous in accordance with our record retention obligations and practices. In the event that we cannot provide you with access to your personal information, we will endeavor to inform you of the reasons why, subject to any legal or regulatory restrictions.

Account Deletion

We hope you will love using Blooket now and always. However, if for some reason you ever want to delete your account, you can do that by contacting us at contact-us@blooket.com and we will proceed to delete the requested data within a reasonable period of time. Parents, legal guardians, or eligible students may delete their accounts by contacting their educational institution. When we delete your account, we delete any personal information that you provided in your profile (such as your name, username, password, and email address) and also questions, responses and comments. Please note that information that you have shared with others, that others have shared about you, or content other users may have copied and stored, is not part of your account and may not be deleted when you delete your account. Part of your personal information will remain in our possession as a copy or backup that is part of our disaster recovery storage system for such period of time identified in our data retention policy.

Consumer Complaints

You may file a complaint concerning Blooket's processing of your personal data to contact-us@blooket.com or by regular mail to the following address: Blooket LLC, 409 South Ridge Avenue, Middletown, DE 19709 USA.

We will take steps to remedy issues arising out of Blooket's alleged failure to comply with the principles set out in this Privacy Policy. We will respond to your complaints within thirty (30) days. If your complaint cannot be resolved through our internal processes, we will direct you to the state or national data protection authority in the jurisdiction where you reside.

EEA Residents

EEA residents and residents from the United Kingdom (UK) will have the right to lodge a complaint to the EU Data Protection Authorities or the Swiss Federal Data and Information Commissioner (FDPIC), Blooket will comply with the advice of competent European Union authorities in such cases, and will provide appropriate recourse. Blooket is also subject to the investigatory and enforcement powers of the US Federal Trade Commission.

Liability

In the event that Blooket or the aforementioned authorities determine that Blooket failed to comply with this policy, Blooket will take appropriate steps to address any adverse effects arising directly from such failure and to promote future compliance.

Europe

As part of a global organization, Blooket operates both within and outside the European Economic Area (the "EEA") and from time to time we may transfer your data from the EEA for processing in a territory outside the EEA that does not have the same statutory levels of data protection as the EEA. Residents in the European Union are entitled to certain rights with respect to personal information that we hold about them:

- **Right of access and portability.** The right to obtain access to your personal information, along with certain related information, and to receive that information in a commonly used format and to have it transferred to another data controller;
- **Right to rectification.** The right to obtain rectification of your personal information without undue delay where that personal information is inaccurate or incomplete;
- **Right to erasure.** The right to obtain the erasure of your personal information without undue delay in certain circumstances, such as where the personal information is no longer necessary in relation to the purposes for which it was collected or processed;
- **Right to restriction.** The right to obtain the restriction of the processing undertaken by us on your personal information in certain circumstances, such as where the accuracy of the personal information is contested by you, for a period enabling us to verify the accuracy of that personal information; and

- **Right to object.** The right to object, on grounds relating to your particular situation, to the processing of your personal information, and to object to processing of your personal information for direct marketing purposes, to the extent it is related to such direct marketing.

You may also have the right to make a complaint to the relevant Supervisory Authority. If you need further assistance regarding your rights, please contact us and we will consider your request in accordance with applicable law. In some cases, our ability to uphold these rights for you may depend upon our obligations to process personal information for security, safety, fraud prevention reasons, compliance with regulatory or legal requirements, or because processing is necessary to deliver the services you have requested. Where this is the case, we will inform you of specific details in response to your request.

California

California AB 1584

Regarding California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1), Blooket will adhere to the following:

- Student records obtained by Blooket from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights of the personal information and education records it provides to Blooket.
- Blooket users may retain possession and control of their own generated content by signing into and accessing their Blooket account and deleting, where applicable, modifying or updating their information within Blooket.
- Blooket will not use any information in a student record for any purpose other than those required or specifically permitted by Blooket's Terms of Use and Privacy Policy.
- Parents, legal guardians, or eligible students may review personally identifiable information in the student's records and correct erroneous information by contacting their educational institution. Additionally, Blooket users may access, correct, update, or delete personal information in their profile by signing into Blooket, accessing their Blooket account, and making the appropriate changes.
- Blooket is committed to maintaining the security and confidentiality of student records. Towards this end, we take the following actions: (a) we limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities; (b) we conduct background checks on our employees that may have access to student data; (c) we conduct regular employee privacy and data security training and education; and (e) we protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.

- In the event of an unauthorized disclosure of a student's records, Blooket will (1) promptly notify users unless specifically directed not to provide such notification by law enforcement officials. Notification shall identify: (i) the date and nature of the unauthorized use or disclosure; (ii) the Private Data used or disclosed; (iii) a general description of what occurred including who made the unauthorized use or received the unauthorized disclosure; (iv) what Blooket has done or shall do to mitigate any effect of the unauthorized use or disclosure; (v) what corrective action Blooket has taken or shall take to prevent future similar unauthorized use or disclosure; and (vi) who at Blooket the user can contact. Blooket will keep the User fully informed until the incident is resolved.
- Blooket will delete or de-identify personal information when it is no longer needed, upon expiration or termination of our agreement with an educational institution with any deletion or de-identification to be completed according to the terms of our agreement with the educational institution, or at the direction or request of the educational institution.
- Blooket agrees to work with educational institutions to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described in statement (4) above.
- Blooket prohibits using personally identifiable information in student records to engage in targeted advertising.

New York

New York Ed. Law § 2-D

In compliance with the requirements set forth in New York Education Law § 2-D, Blooket shall incorporate a Data Privacy and Security Plan ("DPSP") to each contract or other written agreement it enters into with an educational agency from the State of New York. Such DPSP shall outline how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the agreement, consistent with the educational agency's policy on data security and privacy. Such plan shall also include, but shall not be limited to, a signed copy of the parents' bill of rights for data privacy and security, which shall be provided by the educational agency prior to the commencement of the agreement, and a requirement that any officers or employees of Blooket and its assignees who have access to student, teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access. In attention to the foregoing, Blooket hereby commits to:

- (1) limit internal access to education records to those individuals that are determined to have legitimate educational interests (e.g., Blooket employees or third-party service providers);
- (2) not use the education records for any other purposes than those explicitly authorized in the Agreement (i.e., our Terms of Service and this Privacy Policy);

- (3) except for authorized representatives of Blooket to the extent they are carrying out the agreement, not disclose any personally identifiable information to any other party: (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and Blooket provides a notice of the disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- (4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
- (5) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5; and
- (6) notify the educational agency, in the most expedient way possible and without unreasonable delay, of any breach of security resulting in an unauthorized release of student, teacher or principal data, as outlined in applicable State and Federal laws.

Other Countries

Transfers of Personal Information to the U.S.

Blooket is hosted in the United States. If you use the Service from any other regions with laws governing data collection, protection and use that may differ from United States law, please note that you may be transferring your personal information outside of those jurisdictions to the United States. By using the Service, you consent to this, and to the use and storage of personal information in accordance with this Privacy Policy. Third parties that have content embedded on the Blooket website, such as a social feature, may set cookies on a user's browser and/or obtain information about the fact that a web browser visited the Blooket website from a certain IP address. Third parties cannot collect any other personally identifiable information from Blooket's websites unless you provide it to them directly.

Processing in Other Regions

For users from other countries, Blooket will make sure that all appropriate physical, technical and organizational safeguards are adopted in accordance with this Privacy Policy against accidental, unauthorized or unlawful destruction, loss alteration, disclosure, access, use or processing of users' personal information in Blooket's possession.

EXHIBIT "G"**Supplemental SDPC State Terms for [State]**

Version _____

[The State Supplement is an *optional* set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"**) in a separate vendor modified agreement upon request.

EXHIBIT "H"

Additional Terms or Modifications

Version 10/15/2021

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

"LEA and Provider agree that Provider will be able to retain Student Data for legal purposes including but not limited to statutory authority as well as compliance with Court Orders and responding to subpoenas. Student data to be deleted upon the expiration of this agreement shall be specifically identified by the LEA for deletion by the Provider. Upon notice from the LEA of specific Student Data that was provided by the LEA to Provider under accounts created by the LEA, Provider shall delete such data within a commercially reasonable period of time. This Agreement only applies to Student Data transferred pursuant to express agreements between the LEA and Provider."