SCREENCASTIFY STUDENT DATA PRIVACY ADDENDUM

This Student Data Privacy Addendum ("**DPA**") is effective as of the date of full execution or the date of the relevant Screencastify sales order form or other ordering document in which this DPA is incorporated ("**Sales Order**") and is intended to supplement such Sales Order or other services agreement ("**Primary Agreement**") between Screencastify, LLC ("**Screencastify**") and the school district, individual school or other school district partner or agent identified in the Sales Order in which this DPA is incorporated or as identified on the signature line below ("**Local Education Agency**" or "**LEA**").

Whereas, Screencastify and LEA recognize the need to protect Student Data (as defined herein) exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**"), the Children's Online Privacy Protection Act ("**COPPA**") and other state laws that apply based on LEA's jurisdiction (for example, New York State Education Law Section 2-d), and

Whereas, Screencastify and LEA desire to supplement the Primary Agreement with this DPA to establish their respective obligations and duties to comply with applicable laws and regulations.

Therefore, Screencastify and LEA agree as follows:

1. PURPOSE AND SCOPE

a. **Purpose of DPA**. The purpose of this DPA is to describe each Party's duties and responsibilities to protect Student Data. In performing the services as further described in the Primary Agreement (the "**Services**"), Screencastify will be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Screencastify is under the direct control and supervision of the LEA with respect to its use of Student Data.

b. **Description of Services**. As further described in the Primary Agreement, the Services Screencastify provides may include video recording, editing and submission software tools and services designed for use in classroom education settings. Students may be directed by their teachers to create and submit video and audio recordings as part of various classroom assignments, which may be hosted by Screencastify or the LEA's classroom management platform (e.g., Google Classroom).

c. **Student Data to be Provided**. In order for Screencastify to provide its services, the Student Data LEA will provide to Screencastify in connection with the Services may include the following:

  i. Application technology Metadata (e.g., user IP Addresses);

  ii. Application use statistics (e.g., Metadata on user interaction with Screencastify's application);

  iii. Student contact information (e.g., student email address may be collected depending on the selected admin options)

  iv. Student work (e.g., student generated content such as videos generated with the Screencastify application as part of classroom assignments).

d. **Defined Terms**. Defined terms in this DPA have the definitions in **Exhibit A** or as otherwise defined in this DPA. If there is a conflict, the definitions used in this DPA will prevail over definitions in the Primary Agreement.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

a. **Student Data Property of LEA**. All Student Data transmitted to Screencastify pursuant to the Primary Agreement is the property of and under the control of LEA. Screencastify further acknowledges

and agrees that all copies of such Student Data transmitted to Screencastify, including any modifications or additions or any portion thereof, are subject to 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 the Student Data contemplated per the Primary Agreement, will remain the exclusive property of the LEA. Notwithstanding the above, for purposes of FERPA, Screencastify will be considered a School Official under the control and direction of the LEA as it pertains to the use of Student Data.

      b.   **Parent Access**. To the extent required by law, the LEA must establish reasonable procedures by which a parent, legal guardian or eligible student may review Education Records and/or Student Data, correct erroneous information or transfer student-generated content to a personal account consistent with the functionality of the Services. Screencastify must respond in a timely manner (no later than forty-five (45) days from the date of the request or pursuant to the time frame required under applicable 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 Screencastify to view or correct as necessary. If a parent of a student or other individual contacts Screencastify to review any of the Student Data accessed pursuant to the Services, Screencastify must refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

      c.   **Law Enforcement Requests**. If a law enforcement or other government entity ("**Requesting Party**") contacts Screencastify with a request for Student Data held by Screencastify pursuant to the Services, Screencastify must notify LEA in advance of a compelled disclosure to the Requesting Party unless the Requesting Party lawfully directs Screencastify not to inform LEA of the request.

      d.   **Subprocessors**. Screencastify must ensure all Subprocessors performing functions for Screencastify that involve processing of Student Data protect Student Data consistent with this DPA.

3. LEA DUTIES

      a.   **Provide Data in Compliance with Applicable Laws**. LEA must 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.

      b.   **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA, 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.

      c.   **Reasonable Precautions**. LEA must take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

      d.   **Unauthorized Access Notification**. LEA must notify Screencastify promptly of any known unauthorized access to Student Data. LEA will assist Screencastify in its efforts to investigate and respond to any unauthorized access.

      e.   **Consent to Collect Student Data**. LEA represents and warrants that it has (i) the authority to consent to Screencastify's collection and use of personal information from its students; (ii) obtained any required parental consent for Screencastify's collection and use of personal information from its students, including if required verifiable parental consent under COPPA; and (iii) not received any revocation of parental consent. By enrolling a student or helping the student use the Services, LEA provides consent to Screencastify for the collection and use of its students' personal information solely in connection with the use of the Services for classroom educational purposes

4. SCREENCASTIFY DUTIES

      a.   **Privacy Compliance**. Screencastify must comply with all applicable federal, state and local laws, rules and regulations pertaining to Student Data privacy and security.

b. Authorized Use. Screencastify must not use Student Data shared pursuant to the Primary Agreement, including any persistent unique identifiers if applicable, for any purpose other than to provide the Services or as otherwise authorized in the Primary Agreement or this DPA. Screencastify must not sell or rent Student Data to any third party for any purpose.

c. Screencastify Employee Obligations. Screencastify must require its employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to Student Data shared under the Primary Agreement. Screencastify agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data shared under the Primary Agreement. Screencastify will conduct appropriate training of its employees who will access and handle Student Data on legal obligations and best practices with respect to Student Data.

d. No Disclosure. Screencastify must not disclose any Student Data or any portion thereof, including user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by LEA, this DPA or the Primary Agreement. This non-disclosure obligation does not apply to (i) De-Identified information, (ii) Student Data disclosed pursuant to a lawfully issues subpoena or other legal process, or (iii) Subprocessors performing services on Screencastify's behalf pursuant to the Primary Agreement and subject to this DPA.

e. De-Identified Data. Screencastify agrees not to attempt to re-identify de-identified Student Data. Screencastify may use De-Identified Data 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 Screencastify'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. Screencastify's use of De-Identified Data will survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Screencastify 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, Screencastify shall obtain the LEA's written approval of the manner in which de-identified data is presented.

f. Disposition of Data. Upon written request from LEA, Screencastify must dispose of Student Data obtained under the Primary Agreement within sixty (60) days of the request. Screencastify's duty to dispose of Student Data does not apply to De-Identified Student Data.

g. No Student Advertising. Screencastify must not use, disclose or sell Student 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 Services to LEA. This section does not prohibit Screencastify from using Student Data for (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.

5. DATA SECURITY

a. Data Security. Screencastify agrees to employ reasonable administrative, physical and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use or modification. Screencastify must adhere to any applicable laws related to data security. Screencastify will endeavor to maintain a cybersecurity framework based on NIST Cybersecurity Framework Version 1.1 and will employ encryption methods to student data while in transit and at rest in accordance with applicable laws and education industry standards.

b. Audits. No more than once per year, or following a Student Data security breach, and upon written request from LEA with at least fifteen (15) business days' advance written notice and upon the execution of an appropriate non-disclosure agreement, Screencastify will allow 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 the Services to LEA.

      c. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of LEA's Student Data maintained by Screencastify, Screencastify will provide notification to LEA within seven (7) days of confirmation that the incident impacted LEA's Student Data, unless such notification would disrupt investigation of the incident by law enforcement in which case Screencastify will notify LEA as soon as is reasonably practicable. Screencastify and LEA will adhere to the following process with respect to such notification:

      i. The security breach notification described above must include at least the following information if known by Screencastify and as it becomes available:

        1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

        2. If possible to determine, either (1) the date of the breach, (2) the estimated date of the breach or (3) the date range within which the breach occurred;

        3. A general description of the breach incident if that information is possible to determine at the time notice is provided.

      ii. Screencastify must comply with all applicable federal and state requirements with respect to any data breach related to LEA's Student Data, including, as required, the responsibilities and procedures for notification and mitigation of any such data breach.

      iii. Screencastify must have a written incident response plan that reflects best practices and is consistent with industry standards among organizations similar to Screencastify and as required by federal and state law for responding to data breaches and privacy incidents.

      iv. LEA is responsible for providing notice and facts surrounding the breach to any affected students, parents or guardians as may be required by law or policy, provided however, that Screencastify must reimburse LEA for the full cost of such notification to the extent required as a result of the unauthorized release of Student Data by Screencastify or its Subprocessor.

      v. If the breach originates from LEA's use of the Services, Screencastify agrees to cooperate with LEA to the extent necessary to expeditiously secure LEA's Student Data.

6. WARRANTIES AND LIABILITY

      a. **LIMITATION OF LIABILITY.** EXCEPT FOR SCREENCASTIFY'S OBLIGATIONS UNDER SECTION 5(C)(IV), UNDER NO CIRCUMSTANCES WILL EITHER PARTY BE LIABLE FOR INDIRECT, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES (EVEN IF THAT PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) INCLUDING ANY LOSS OF REVENUE, PROFITS OR DATA ARISING OUT OF OR RELATED TO THIS DPA. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, EXCEPT FOR CLAIMS BASED ON SCREENCASTIFY'S WILLFUL MISCONDUCT, SCREENCASTIFY'S AGGREGATE LIABILITY ARISING OUT OF OR WITH RESPECT TO THIS DPA IS LIMITED TO THE TOTAL AMOUNTS PAID BY CUSTOMER UNDER, OR IN CONNECTION WITH THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH CLAIM OR $500, WHICHEVER IS LESS.

      b. **Warranties.** Except as set forth in the Primary Agreement or this DPA, Screencastify makes no representations or warranties as to the quality or reliability of the Services and to the maximum extent permitted by applicable law, the Services are provided on an "as-is" basis and Screencastify disclaims all implied or statutory warranties (including claims about merchantability, title, non-infringement, accuracy, or

fitness for a particular purpose). Customer acknowledges Screencastify does not control and Screencastify is not responsible for any interruptions, delays, cancellations, delivery failures, data loss, content corruption, packet loss, or other damage arising from (i) Customer equipment or the transfer of data over communication networks, facilities, and devices (including the Internet); (ii) limitations, interruptions, delays, cancellations, and other problems inherent in the use of such communications networks, facilities, and devices not within Screencastify's control; and (iii) Customer's failure to properly install appropriate security updates and patches to software and programs on networks and devices within Customer's control.

7. MISCELLANEOUS

a. Term/Termination. The term of this DPA will run concurrently with the Primary Agreement and/or any other services agreement or subscription license between Screencastify and LEA. This DPA will terminate automatically upon expiration or termination of such Primary Agreement and/or any other services agreement or subscription license between Screencastify and LEA, provided however, that all provisions of this DPA that, by their nature must survive termination of this DPA, will survive termination and continue to apply to LEA's Student Data.

b. Priority of Agreements. Regarding Student Data, this DPA will control in the event of a conflict with the Primary Agreement or any other agreement between LEA and Screencastify.

c. Governing Law; Venue and Jurisdiction. This DPA will be governed by and construed in accordance with the laws of the state in which LEA is located, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county in which LEA is located for any dispute arising out of or relating to this DPA.

d. 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 will not invalidate or render unenforceable such provision in any other jurisdiction.

e. Successors Bound. This DPA will be binding upon the respective successors in interest to Screencastify 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.

f. Authority. Each party represents it is authorized to bind to the terms of this DPA.

g. 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.

ACCEPTED AND AGREED:

SCREENCASTIFY, LLC	*DocuSigned by:* David Pruitt —028662255AAD440...	LEA:
Signature:		Signature: Kathur Kuye
Name: David Pruitt		Name: Katherine Krueger
Title: General Counsel		Title Director of Technology
Date: 5/18/2022		Date: 10/18/2023

EXHIBIT A

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 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.

Education Records: Education 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.

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.

Student Data: Student Data includes any data, whether gathered by Screencastify or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including 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 section 1(c) of this DPA is confirmed to be collected or processed by Screencastify 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 Screencastify'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 Screencastify, who Screencastify uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

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 website based on the content of the web page or in response to a student's response or request for information or feedback.