

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 has agreed or will agree to provide the LEA with certain digital educational services as described in Section 1 and pursuant to the Primary Agreement, which includes Screencastify’s Master Subscription Terms and Conditions located at www.screencastify.com/msa, which are incorporated herein by reference; and

Whereas, in order to provide the Services (as described below), Screencastify may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“**FERPA**”), the Children’s Online Privacy Protection Act (“**COPPA**”), and the Protection of Pupil Rights Amendment (“**PPRA**”), 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 (as defined in **Exhibit A**). 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. Nature of Services Provided. As further described in the Primary Agreement, the Services Screencastify provides may include video recording, editing and submission software tools and services used in classroom education settings for teachers to create and share video contents. Students may also 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 Drive/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. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from a student’s Education Record to a third party without written consent of the parent and/or eligible student without meeting one of the exemptions set forth in FERPA (“**FERPA Exemption(s)**”), including the exemption for Directory Information or School Official Exemption. For FERPA purposes, to the extent Personally Identifiable Information from Education Records are transmitted to Screencastify from LEA or from students using Screencastify under the direction of LEA, Screencastify shall be considered a School Official under the control and direction of the LEA as it pertains to the use of Student Data. Additionally, certain information provided to Screencastify by LEA about a student may be considered Directory Information (name, email address, grade level, etc.) under FERPA and not an Education Record.

c. **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. Screencastify further acknowledges that LEA is subject to the Parents Bill of Rights attached to this DPA as **Exhibit B** and will cooperate with LEA to meet such requirements.

d. 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.

e. 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 in all material respects with all applicable federal, state and local laws, rules and regulations pertaining to Student Data privacy and security in providing the Services to LEA. Screencastify agrees that it will comply in all material respects with those provisions of the LEA’s Parents Bill of Rights for Data Security and Privacy attached hereto as **Exhibit B**.

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. The foregoing does not apply to De-Identified Data.

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 may use De-Identified Data for any lawful purpose, including 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. Screencastify agrees not to attempt to re-identify De-Identified Data and not to transfer De-Identified Data to any party unless that party agrees in writing not to attempt re-identification.

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 Personally Identifiable Information contained in 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 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. 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 or its assignees (“**Security Incident**”), 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 by applicable law and where the Security Incident is (1) the result of the unauthorized release of Student Data by Screencastify or its Subprocessor and (2) not the result of the LEA’s actions or inactions.
- 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. EDUCATION LAW 2-D SUPPLEMENTAL INFORMATION

- a. In accordance with Education Law section 2-d(3)(c) and Section 121.3 of the implementing Regulations, the attached **Exhibit C** includes the “Supplemental Information” required to be posted on LEA’s website.

7. WARRANTIES AND LIABILITY

a. LIMITATION OF LIABILITY. EXCEPT FOR SCREENCASTIFY'S OBLIGATIONS UNDER SECTION 5(B)(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.

8. 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 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 t, as often as may be deemed expedient.

[Signature Page Follows]

ACCEPTED AND AGREED:

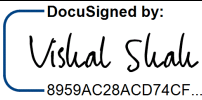
Screencastify, LLC	LEA Cayuga Onondaga BOCES
Signature:  8959AC28ACD74CF...	Signature: <i>Pamela Horton</i>
Name: Vishal Shah	Name: Pamela Horton
Title: CEO	Title: Director of Instructional Support Services
Date: 3/26/24	Date: 5.7.24

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 contractor that: (1) Performs an institutional service 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 Metadata. 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 overtime from the usage of the operator's Internet website, online service or mobile application by such student or the retention of such student's online activities or requests overtime for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to students on an Internet website based on the content of the webpage or in response to a student's response or request for information or feedback.

EXHIBIT B

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-d of the New York State Education Law (“**Education Law 2-d**”), parents and eligible students are entitled to certain protections regarding confidential student information. The School District identified below (the “**District**”) is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below. Any terms not defined herein shall have the meaning set forth in Education Law 2-d or in the Screencastify Student Data Privacy Addendum to which this document is an Exhibit.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
2. A student's personally identifiable information cannot be sold or released for any commercial purposes by a third-party contractor. The district will not sell student personally identifiable information and will not release it for commercial purposes, other than directory information released by the district in accordance with district policy.
3. Parents have the right to inspect and review the complete contents of their child's education record.
4. State and federal laws protect the confidentiality of personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
5. A complete list of all student data elements collected by the State Education Department is available for public review at <http://www.p12.nysed.gov/irs/sirs/>
6. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the address set forth on the signature page of this Exhibit. Complaints can also be directed to the New York State Education Department by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to CPO@mail.nysed.gov.
7. The District has entered into contracts with certain third party contractors who have received Student Data, teacher data and/or principal data. These contracts will include the following: (a) The exclusive purposes(s) for which the Student Data will be used; (b) The commencement and termination dates of each such contract; (c) A description of how parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data or the teacher or principal data that is collected; and (d) The data storage and security measures undertaken for Student Data or teacher or principal data, including whether such data will be encrypted.
8. In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the address set forth on the signature page of this Exhibit.

Name of District: Cayuga Onondaga BOCES

Address: Auburn, NY 13021

District Authorized Representative: Pamela Horton

Title: Director of Instructional Support Services

Signature: *Pamela Horton*

Date: 5.7.24

EXHIBIT C

SUPPLEMENTAL INFORMATION

District and Screencastify have entered into a Student Data Privacy Addendum (“**DPA**”). The DPA supplements the Primary Agreement and together with the Primary Agreement, is collectively referred to as the “**Agreement**.” All terms not defined below or in the DPA shall have the meaning set forth in Education Law 2-d.

As required by Education Law section 2-d(3)(c) and Section 121.3 of the implementing Regulations, the following is the “**Supplemental Information**” for the Agreement with Screencastify.

1. **Purpose of Use.** Screencastify will use PII solely for the purpose of providing products and services to the Customer and as explicitly authorized in its agreement with Customer.
2. **Term and Termination of Primary Agreement:** The Primary Agreement begins and ends on the following dates as specified in the Primary Agreement: June 30, 2026.
3. **Challenges to Accuracy / Deletion Requests.** As provided in Screencastify’s Privacy Policy, if a parent or eligible student wishes to challenge the accuracy of or delete PII that is maintained by Screencastify, that request may be processed through the procedures provided by the Customer for amendment of education records under FERPA and the Customer may notify Screencastify of such request by emailing privacy@screencastify.com.
4. **Deletion of Customer Data.** Screencastify will delete Customer’s PII so that it is physically and virtually irrecoverable within sixty (60) days of LEA’s termination of its services relationship with Provider, and will provide the LEA with confirmation of such deletion upon written request.
5. **Subcontractor Oversight.** Screencastify’s policy is to (i) vet prospective subcontractors and service providers who may handle PII on Screencastify’s behalf to ensure they have acceptable controls in place to protect PII, (ii) only share PII with subcontractors, service providers and other third parties that are contractually bound to observe equally stringent obligations to maintain data privacy and security as are required of Screencastify pursuant to this Plan and (iii) regularly review its service providers with access to PII to ensure they continue to meet the requirements of this Plan.
6. **Security Practices and Procedures.** Screencastify has implemented the following security controls intended to provide reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII in its custody:
 - A. Screencastify has designated a privacy officer responsible for information security governance and maintains privacy policies and practices that support compliance with the Family Educational Rights and Privacy Act (“**FERPA**”), the Children’s Online Privacy Protection Act (“**COPPA**”) and other applicable laws.
 - B. PII is hosted in Google Cloud data centers located in the United States that maintain their own rigorous industry standard certifications and compliance offerings.
 - C. Screencastify will comply with its privacy policy at www.screencastify.com/legal/privacy

- D. All provisions of the Customer's Parents' Bill of Rights for data privacy and security as required by New York Ed Law 2d are incorporated into this Exhibit.
 - E. Screencastify provides regular privacy and security awareness training, including training on applicable laws that govern the handling of PII, to its employees who will have access to PII.
 - F. Screencastify limits internal access to education records and PII to those individuals that are determined to have legitimate educational interests within the meaning of §2-d and FERPA; e.g., the individual needs access to the PII in order to fulfill his or her responsibilities in performing services to the Customer;
 - G. Screencastify uses encryption technology and other suitable means to protect the PII in Screencastify's custody, whether in motion or at rest, from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of Health and Human Services in guidance issued under P.L. 111-5, Section 13402(H)(2), or any other technology or methodology specifically authorized by applicable statute, regulation or the New York State Education Department;
 - H. If Screencastify becomes aware of any breach of security resulting in an unauthorized release of Customer's PII by Screencastify or its subcontractors, Screencastify will notify Customer as required by applicable law or otherwise where Screencastify deems necessary to protect the safety and security of PII.
 - I. Screencastify uses a minimum encryption of AES256 for all data at rest and a minimum of TLS 1.3 for all data in transit.
 - J. Screencastify has dedicated employee resources charged with maintaining necessary and reasonable security controls to protect student data. The company maintains a comprehensive information security policy aligned with the controls set forth in NIST CSF v. 1.1 and relies on a combination of monitoring of data systems (such as vulnerability scans and detection processes) and access controls (for example, least privilege principles) to help ensure the security of data systems.
7. **Further Amendments.** The parties acknowledge that an addendum to this Exhibit may be necessary to ensure compliance with §2-d following the promulgation of any additional regulations and/or the issuance of further guidance by the New York State Education Department subsequent to the execution of the Agreement. The parties agree to act in good faith to take such additional steps to amend this Exhibit as may be necessary at that time.