Version 2.0 Agreement Approved: June 2019

DATA PRIVACY AGREEMENT (DPA)
FOR TEXAS K-12 INSTITUTIONS

Boerne Independent School District March 5, 2025

LEA NAME [Box 1] DATE [Box 2]

and

Screencastify, LLC March 5, 2025

OPERATOR NAME [Box 3] DATE [Box 4]

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency ("LEA") with certaindigital educational services ("Services") according to a contract titled "Master Subscription Terms and Conditions"
[Box 5]
and dated 03/05/25 (tbe "Service Agreement"), and
[Box 6]

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506, and Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

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

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

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

ARTICLE I: PURPOSE AND SCOPE

1. **Nature of Services Provided.** The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement.

2. **Purpose of DPA**. For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties' responsibilities to protect Data.

3. **Data to Be Provided**. In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Exhibit C. In the event ofa conflict, definitions used in this DPA shall prevail over terms used in the ServiceAgreement.

ARTICLE VI- GENERAL OFFER OF PRIVACYTERMS

1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

ARTICLE VII: MISCELLANEOUS

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

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

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

4. **Priority of Agreements**. This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before: The designated representative for the Operator for this Agreement is:

First Name: Caroline [Box 7]

Last Name: Prinske [Box 8]

Operator's Company Name: Screencastify, LLC [Box 9]

Title of Representative: Team Lead [Box 10]

The designated representative for the LEA for this Agreement is:

First Name: Sean [Box 11]

Last Name: Babcock [Box 12]

LEA's Name: Boerne ISD [Box 13]

Title of Representative: Chief Technology Officer [Box 14]

IN WITNESS WHEREOF, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

Operator's Representative:

Signed by:

BY: Caroline Prinske [Box 15] Date: 03/05/25 [Box 16]

3AD7A777D72A47B...

Printed Name: Caroline Prinske [Box 17] Title/Position: Team Lead [Box 18]

Address for Notice Purposes: 333 N. Green St., Suite 810, Chicago, IL 60607 [Box 19]

LEA's Representative

BY: Sean C Babcock [Box 20] Date: 4/1/2025 [Box 21]

Printed Name: Sean Babcock [Box 22] Title/Position: CTO [Box 23]

Address for Notice Purposes: Johns Road, Boerne, Texas, 78 [Box 24]

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Description : [Box 25]

Screencastify provides video recording, editing and sharing software tools and services designed for use in classroom educational settings. Students may be directed by their teachers to create and submit video and audio recordings as part of classroom assignments. Access to the platform is based on a paid subscription, but there is also a free version of the services. All data is stored on services hosted in the United States.

EXHIBIT " B"

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the "Other" category to list the data collected.

□ We do not collect LEA Data to provide the described services.

■ We do collect LEA Data to provide the described services.

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	☒
	Other application technology meta data-Please specify:	□
Application Use Statistics	Meta data on user interaction with application- Please specify:	☒
Assessment	Standardized test scores	□
	Observation data	□
	Other assessment data-Please specify:	□
Attendance	Student school (daily) attendance data	□
	Student class attendance data	□
Communications	Online communications that are captured (emails, blog entries)	□
Conduct	Conduct or behavioral data	□
	Date of Birth	□

Demographics	Place of Birth	□
	Gender	□
	Ethnicity or race	□
	Language information (native, preferred or primary language spoken by student)	□
	Other demographic information-Please specify:	□
Enrollment	Student school enrollment	□
	Student grade level	□
	Homeroom	□
	Guidance counselor	□
	Specific curriculum programs	□
	Year of graduation	□
	Other enrollment information-Please specify:	□
Parent/Guardian Contact Information	Address	□
	Email	□
	Phone	□
Parent/Guardian ID	Parent ID number (created to link parents to students)	□
Parent/Guardian Name	First and/or Last	□
Schedule	Student scheduled courses	□
	Teacher names	□
Special Indicator	English language learner information	□
	Low income status	□
	Medical alerts /health data	□
	Student disability information	□
	Specialized education services (IEP or 504)	□
	Living situations (homeless/foster care)	□
	Other indicator information-Please specify:	□

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	□
	Email	☒
	Phone	□
Student Identifiers	Local (School district) ID number	□
	State ID number	□
	Vendor/App assigned student ID number	□
	Student app username	□
	Student app passwords	□
Student Name	First and/or Last	☒
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.	☒
	Other student work data -Please specify: User generated videos as directed by classroom instructor	☒
Transcript	Student course grades	□
	Student course data	□
	Student course grades/performance scores	□
	Other transcript data -Please specify:	□
	Student bus assignment	□
	Student pick up and/or drop off location	□

	Transportation	Student bus card ID number	□
		Other transportation data -Please specify:	□
	Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	□

EXHIBIT "D"

SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

Instructions: This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

Boerne Independent School District directs Screencastify, LLC to

LEA OPERATOR

dispose of return data obtained by Operator pursuant to the terms of the Service Agreement between LEA and Operator. The terms of the Disposition are set forth below:

1. Extent of Return or Disposition

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

□ Return or Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Return or Disposition

□ Disposition shall be by destruction or deletion of data.

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

3. Timing of Return or Disposition

Data shall be returned or disposed of by the following date:

□ As soon as commercially practicable

□ By the following agreed upon date:

4. Signatures

____________________________________ ____________________

Authorized Representative of LEA Date:

5. Verification of Disposition of Data

____________________________________ ____________________

Authorized Representative of Operator Date:

EXHIBIT " E"

GENERAL OFFER OF PRIVACY TERMS

Instructions: This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should aSubscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and
Boerne Independent School District
and which is dated [03/05/25] to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the eventof:

(1) a material change in the applicable privacy statutes;
(2) a material change in the services and products listed in the Originating ServiceAgreement;
(3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.

Operator's Representative:

Signed by:
BY: Caroline Prinske
3AD7A777D72A47B...

Date: 03/03/25

Printed Name: Caroline Prinske

Title/Position: Team Lead

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

Subscribing LEA's Representative:

BY: Sean C.

Date: 4/1/2025

Printed Name: SEAN Babcock

Title/Position: CTO

EXHIBIT "F"

DATA SECURITY

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

Caroline Prinske [Box 26]
Named Security Contact

caroline.prinske@screencastify.com [Box 27]
Email of Security Contact

(224) 419-7836 [Box 28]
Phone Number of Security Contact

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

https://learn.screencastify.com/hc/en-us/articles/360049157034-Who-do-you-share-my-data-with [Box 29]

3. **Additional Data Security Measures:**

[Box 30]

Screencastify

ADDENDUM TO DATA PRIVACY AGREEMENT

This Addendum supplements and modifies the Student Data Privacy Agreement ("**DPA**") to which it is attached between Screencastify, LLC ("**Screencastify**") and the applicable school district or local education agency ("**LEA**") as such DPA applies to certain software and services Screencastify provides to LEA (the "**Services**").

Screencastify and Customer agree to incorporate the following terms into the DPA:

1. **Provider MSA Terms**. Screencastify's Services are subject to Screencastify's Master Subscription Terms and Conditions located at www.screencastify.com/msa ("MSA Terms") and and such MSA terms are incorporated into the DPA, provided that if there is a direct conflict between the MSA Terms and the DPA, the DPA controls.

2. **Breach Notification**. The timeframe for any notification Screencastify is required to provide to LEA in connection with any unauthorized disclosure of personally identifiable information is within seven (7) days following Screencastify's confirmation of such incident related to LEA's personally identifiable information.

3. **Data Security and Privacy Plan.** To the extent the DPA requires Screencastify to submit supplemental information and/or a data security and privacy plan the attached Data Security and Privacy Plan is incorporated into the DPA.

Screencastify

DATA SECURITY AND PRIVACY PLAN

Updated July 27, 2023

This Data Security and Privacy Plan (this "Plan") has been implemented and will be maintained by Screencastify, LLC ("Screencastify") in compliance with all applicable laws, including the New York Education Law §2-d ("§2-d") and regulations promulgated thereunder.

Screencastify will undertake industry standard practices, including physical controls, firewalls, and password protection, to protect the privacy and security of personally identifiable information ("PII") that Screencastify receives under each agreement (the "Agreement") with an educational agency customer subject to §2-d (the "Customer"), including alignment with the requirements of the National Institute for Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

Screencastify will keep confidential all PII to which it has access in the performance of the Agreement. In addition to the above requirements, for PII:

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. **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.

3. **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.

4. **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.

5. **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 https://www.screencastify.com/privacy/policy.

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 Plan.

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.

6. **Further Amendments.** The parties acknowledge that an addendum to this Plan 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 Plan as may be necessary at that time.

7. **NIST CSF Alignment.** The following chart demonstrates how Screencastify's information security program materially aligns with the NIST Cybersecurity Framework version 1.1.

Screencastify

EXHIBIT 1 – NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	All devices, systems and facilities that enable the organization to achieve business purposes are carefully and diligently utilized and managed by board certified and licensed therapists who adhere to strict scopes of practice, ethical standards. Risk management team is put in place to assess and identify breach or security threat and will be handled in a systematic order to identify, assess, report and review any breach and to ensure there is no recurrence.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The mission, objectives, stakeholders and activities of the business are understood by all functioning members of the business and this information is regularly presented to each involved team member and reviewed in case of breach in order to review risk management decisions and processes
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are presented frequently and inform the steps and process of handling and avoiding cybersecurity risks
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Yes, the organization understands all ramifications of cybersecurity risks and attacks. The organization has risk management assessment in place to ensure security. Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	All organization risk management strategies are identified, established, assessed, managed and agreed to by all team members
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	All organization risk management strategies are identified, established, assessed, managed and agreed to by all team members
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Physical access to assets is managed and protected by authorized user.

	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Contractor's employees, officers, and/or subcontractors are trained and bound by the data protection and security requirements as a "Third-Party Contractor" as outlined in 8 NYCRR Part 121, in accordance with EA's Parents Bill of Rights and Supplemental Information to the Service Agreement
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data is protected when in use and not in use
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Policies and regulations are in place regarding the use, management and oversight of information systems and assets
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and repairs are performed in a secure way that prevents unauthorized access
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Communications and control networks are protected
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Events are identified and assessed.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Vulnerability scans are performed.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes are reviewed and modified for improvement
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Response planning is executed during and after incident to avoid recurrence
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	All team members understand roles when risk response is needed.

	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	All analysis is understood and processes are put in place to receive vulnerabilities and breach reports.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents will be contained, mitigated and kept on alert for risk
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response strategies are continuously reviewed.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery plan is performed during and after incident while strategies and procedures are continuously reviewed and updated.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	strategies and procedures are continuously reviewed and updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Restoration activities include all parties involved in incident