Contract No. C21-353

BOARD APPROVED
DATE 2-11-2021

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:

Pleasanton USD

AND

Provider:

Pixton Comics Inc.

Date:

January 25, 2021

Term: 1/25/2021 - 1/25/2024

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Pleasanton USD

(hereinafter referred to as "LEA") and Pixton Comics Inc. (hereinafter referred to as "Provider") on January 25, 2021 . The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated January 25, 2021 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

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

Web app for making comic strips. Available at https://edu.pixton.com

3. **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. **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 term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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 pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to

attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

    a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

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

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. **Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Coordinator**. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance

monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting 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.
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.
ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

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

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

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is

provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Janet Wolfinger
Title: Coordinator, Purchasing, Warehouse & Graphics

Contact Information:
purchasing@pleasantgrovut.net

The designated representative for the Provider for this Agreement is:

Name: Clive Goodinson
Title: CEO

Contact Information:
clive@pixton.com

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

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

Name: Clive Goodinson
Title: CEO

Contact Information:
Clive Goodinson clive@pixton.com

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and

either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, 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 THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Successors Bound**. This DPA is and shall be binding upon 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.

[Signature Page Follows]

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

Provider: Pixton Comics Inc.

BY: _____ Date: Jan 25, 2021

Printed Name: Clive Goodinson Title/Position: CEO

Local Education Agency: Pleasanton USD

BY: _____ Date: 1/25/2021

Printed Name: Janet Wolfinger Title/Position: Coordinator Purchasing, Warehouse & Graphics

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

Quickly create illustrated comics, storyboards, and custom characters. For educators and students. Fun and easy to use, and sure to engage.

Students will all love writing and being creative with Pixton — whether you're looking to engage reluctant writers, wrap up a special unit, or simply give your students a fun treat.

Students log in and start by creating their avatar. There's even a class photo included for free in all accounts.

Here are a few ways Pixton is used:
- Explaining STEM concepts
- Social stories
- Math word problems
- Creative writing
- Religious studies

For further product information and support, see https://help.pixton.com

See attached document,
Pixton Data Collection - Teachers and Students.pdf

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.	
	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 that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	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:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/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:	
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	

No Student Data Collected at this time _____.
*Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space needed.

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

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

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

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

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

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

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

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

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

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

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Pleasanton USD directs Pixton Comics Inc. 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:

Extent of Disposition Disposition shall be:	____ Partial. The categories of data to be disposed of are as follows: X ____ Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	X ____ Destruction or deletion of data. ____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	____ As soon as commercially practicable X _____By (Insert Date) _____ 60 days after account termination

[signature] 1/27/2021
Authorized Representative of LEA — Date

[signature] Jan 25, 2021
Verification of Disposition of Data by Authorized Representative of Provider — Date

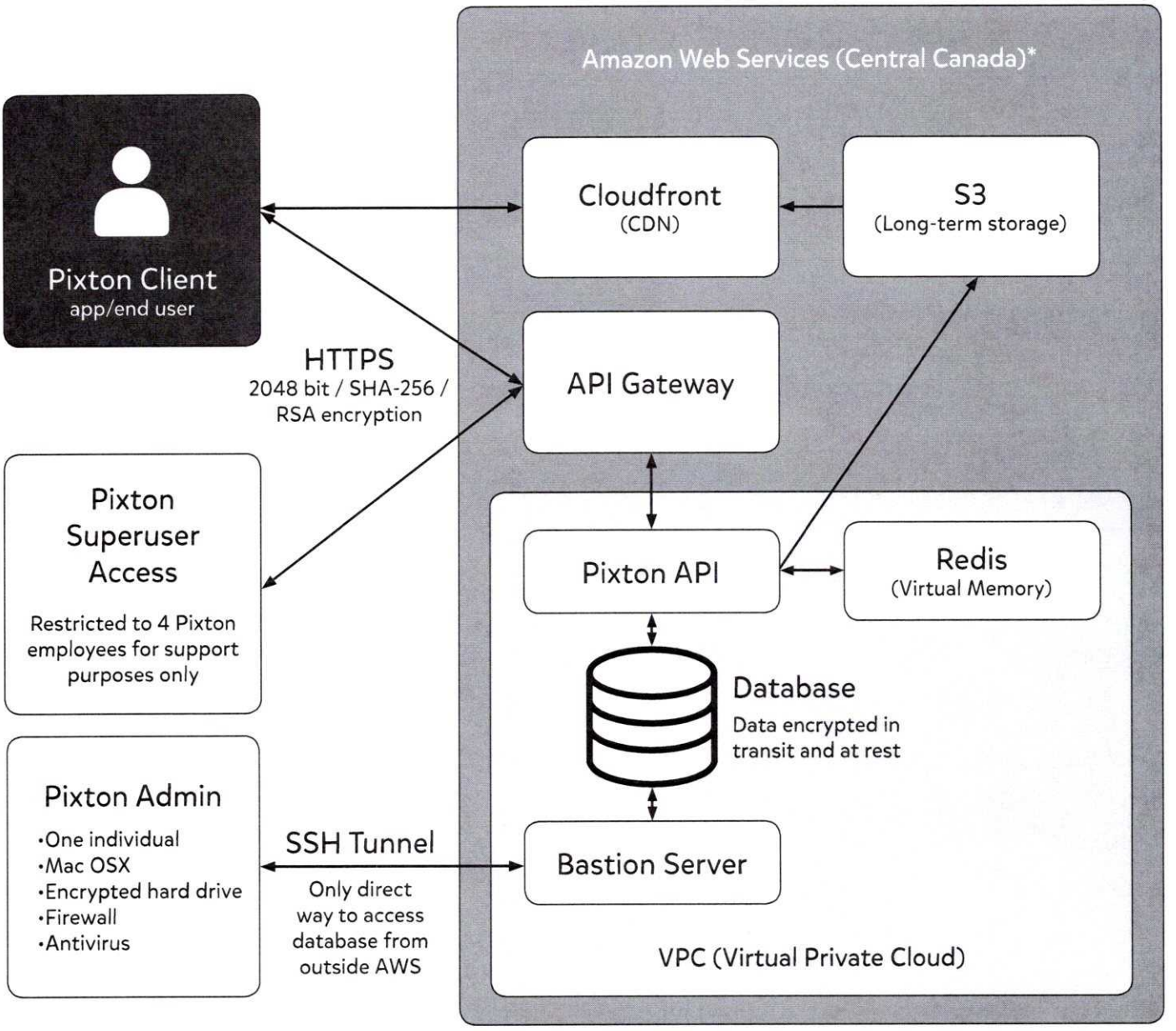
EXHIBIT "F" DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

See attached documents:
Pixton Comics Security Policy.pdf
Pixton Data Collection - Teachers and Students.pdf
Pixton Data Flow Diagram.pdf

PIXTON

Data Flow Diagram



*For simplicity, certain details of Pixton's AWS architecture are not shown, such as security groups.

All data is stored and secured using industry standard access control and encryption. No user data is stored locally.

No comic is displayed publicly, and can only be seen by others if the author shares a link to it. A small number of Pixton personnel are authorized to access comics for customer support purposes only.

Account login is handled strictly via Google, Microsoft or Facebook, so there are no passwords stored in our database. Direct access to the database is only possible through the heavily guarded Pixton Admin.

Prepared on August 26, 2019 by Clive Goodinson (privacy@pixton.com)

Pixton Comics – Security Policy

About this Policy

In supporting our customers and users in general, we deal with personal and/or sensitive information on a regular basis. We collect it through our web app; we store it in places including AWS and Zoho CRM. We sometimes need to look something up in order to respond to a request from a user. Or we may use the information to inform what improvements we make to Pixton.

We also deal with sensitive internal information – the inner workings of Pixton's own systems, and other details about our business.

It is our collective responsibility to keep this information, referred to from here on as Protected Information, safe from accidental or intentional unauthorized disclosure or modification.

This protection includes an appropriate level of security over the software and hardware used to collect, process, store, and transmit Protected Information.

Who Is Affected By This Policy

This Security Policy applies to all employees of Pixton Comics Inc. (the "Company"), as well as to any other individuals and entities granted use of Protected Information, including but not limited to: contractors, temporary employees, and volunteers (collectively, "Staff").

It is the responsibility of the Company's Privacy Officer, Clive Goodinson <privacy@pixton.com>, to communicate this policy, and any changes to it, to all Staff, and to review it at least once every 12 months for compliance, completeness, and accuracy.

Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

Protected Information – information that the Company collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Information Security

The Company appropriately secures its information from unauthorized access, loss or damage while enabling its Staff to support users, plan content creation, and troubleshoot technical issues.

Classification Levels

All Protected Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

The classifications levels are:

Forbidden

The following Protected Information is classified as Forbidden:

- credit card numbers
- user account passwords

Forbidden information must never be collected, communicated, shared, or otherwise used in any way by Staff.

All credit card transactions are handled by Stripe. We cannot accept credit card numbers by phone, email, or any other means.

All primary users of Pixton EDU and Pixton PRO can only use Single Sign-on (SSO) to access their accounts, so we do not store their passwords, even in an encrypted form.

Some students, by the choice of their teacher, will access their accounts using passwords. The passwords are stored in a hashed form in our database, and there should never be a reason to share or attempt to access or decipher said passwords.

Confidential

Protected Information is classified as Confidential if it is not intended to be shared freely within or outside the Company due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include:

- all user information, such as contents of comics, or last 4 digits of credit card;
- workflows facilitated by Pixton's internal content management system;
- internal financial data.

Sharing of Confidential information may be permissible if necessary to meet the Company's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside the Company, the proposed recipient must agree:

- to take appropriate measures to safeguard the confidentiality of the information;
- not to disclose the information to any other party for any purpose absent the Company's prior written consent or a valid court order or subpoena; and
- to notify the Company in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification.

In addition, the proposed recipient must abide by the requirements of this policy.

Unrestricted Within the Company

Protected Information is classified as Unrestricted Within the Company if it falls outside the Forbidden and Confidential classifications, but is not intended to be freely shared outside the Company.

The presumption is that such information will remain within the Company. However, this information may be shared outside of the Company if necessary to meet the Company's legitimate business needs, and the proposed recipient agrees not to re-disclose the information without the Company's consent.

Examples of this type of information include:

- details of Pixton's internal content management system; or
- new features we're working on and seeking feedback on from select users.

Publicly Available

Protected Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of the Company. An example of this type of information is:

- content we've published on our website or elsewhere publicly, eg. content packs, backgrounds, blog posts, etc.

Protection, Handling, and Classification of Information

Based on its classification, Protected Information must be appropriately protected from unauthorized access, loss and damage.

Handling of Protected Information from any source other than the Company may require compliance with both this policy and the requirements of the individual or entity that created, provided or controls the information. If you have concerns about your ability to comply, consult the Company's Privacy Officer.

Responsibilities

All Staff are expected to:

- Understand the information classification levels defined in the Security Policy.
- As appropriate, classify the information for which one is responsible accordingly.
- Access information only as needed to meet legitimate business needs.
- Not divulge, copy, release, sell, loan, alter or destroy any Protected Information without a valid business purpose and/or authorization.
- Protect the confidentiality, integrity and availability of Protected Information in a manner consistent with the information's classification level and type.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access Protected Information.
- Discard media containing Company information in a manner consistent with the information's classification level, type, and any applicable Company retention requirement. This includes information contained in any hard copy document (such as a memo or report) or in any electronic, magnetic or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).
- Contact the Company's Privacy Officer prior to disclosing information generated by the Company or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.

- Contact the Company's Privacy Officer prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

Retention of Information

Protected Information need only be stored as long as there's a conceivable need for it. The retention period of some information (i.e. user information collected through our website) is explicitly defined in our Privacy Policies (see https://edu.pixton.com/educators/privacy-policy; https://pro.pixton.com/business/privacy-policy). Otherwise, it is the responsibility of each Staff member to use their best judgement in determining how long information should be kept and when to archive or delete it.

Periodic Review

At a minimum, this Security Policy will be reviewed for compliance, completeness and accuracy every 12 months.

Acceptable Use

The goal of this document is not to impose restrictions that are contrary to the established culture of openness, trust and integrity of the Company, but to protect Staff from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Staff member who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

These guidelines apply to the use of information, electronic and computing devices, and network resources to conduct Company business or interact with internal networks and business systems, whether owned or leased by the Company, a Staff member, or a third party.

You may access, use or share Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Always exercise good judgment regarding the reasonableness of personal use.

Use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

- Don't use copyrighted material that we aren't licensed to use.
- Don't use any Company data, account, or equipment for any purpose other than Company business.
- Do not share your password or other authentication details with anyone, unless expressly authorized to do so. If you do share such information, only do so via sanctioned means (eg. LastPass).
- Do not provide information about, or lists of, Staff to parties outside the Company.

Passwords

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

You must use LastPass (https://www.lastpass.com/) to store, retrieve, and share all user-level and system-level passwords, unless otherwise expressly permitted by the Privacy Officer.

Passwords must:

- be eight or more characters long;
- include at least one lower-case letter, one upper-case letter, one number, and one special character (i.e. neither number nor letter);
- not contain guessable patterns (e.g. "password123") or personal information (e.g. your birthdate);
- use a separate, unique password for each work-related account.

In addition:

- Work-related passwords may not be used for personal accounts, and vice-versa;
- Multi-factor authentication must be used for access to production environments (eg. Amazon Web Services console);
- Passwords should be changed if there is reason to believe a password has been compromised;
- Passwords must not be shared with anyone, including supervisors and coworkers, unless expressly permitted by the Security Officer;
- If you suspect your password has been compromised in any way, you must change all passwords and report the incident immediately to the Privacy Officer.

Application Development

In developing our own applications and using third-party applications, accounts must always be created for individuals, and not for groups. In addition:

- Applications must not store passwords in clear text or in any easily reversible form;
- Applications must not transmit passwords in clear text over the network;
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Incident Response Process and Procedures

Any security incident must be reported immediately to the Company's Privacy Officer, who is responsible for diagnosing and resolving the issue, and reporting it to any other appropriate parties.

Social Engineering

One of the most popular and effective methods of gaining unauthorized access to Protected Information is social engineering – the art of manipulating people so they give up confidential information.

It is important to know when and when not to take a person at their word and when the person you are communicating with is who they say they are.

Email

Be wary of any links, files, or other attachments you receive by email. If the link is a URL, hover over it first to see what URL it actually links to. If you don't recognize and trust the domain, or if the domain of the link doesn't match the link text, don't follow the link. Never open any file sent to you by email, unless you are expecting it and it's from a trusted source. It's possible for criminals to create links and files that, if opened on your computer can take over your machine, resulting in theft of data, collection of your contacts' information, and other nefarious deeds.

Software Installation

Seek permission before installing any new software on a computing device on which Protected Information is stored or may be accessed.

Be sure to turn on disk encryption on your devices, as well as password protection and automatic timeout to screensaver.

Vulnerability Scans and Code Reviews

All code and software developed by the Company must be scanned for vulnerabilities, both as part of our ongoing development work, and periodically system-wide. This applies to both front-end web clients and back-end server APIs.

Code and software interfaces must be reviewed at least once a year, or whenever a new major version is to be released, using the OWASP Top 10 vulnerabilities (see https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf) as a guide. Vulnerability scans can be performed through code review, or via vulnerability scanning software such as Wapiti (see http://wapiti.sourceforge.net/).

Results of Code Review, September 2019

All proprietary code and APIs were reviewed in September 2019, according to the OWASP Top 10 vulnerabilities. Here are the results:

1. Injection

- All (MySQL) query values are escaped using the '?' placeholder (see https://github.com/mysqljs/mysql#escaping-query-values)

2. Broken authentication

- Pixton uses only single sign-on (OAuth 2.0) with Google, Facebook, and Microsoft for primary account holders.
- User session data is deleted from local storage on logout, or times out after a period of inactivity.
- All entity IDs are non-sequential 20-digit integers; all access tokens are complex and unguessable.

3. Sensitive data exposure

- The only sensitive data stored is the user's email address, display name, and the content of their comics and related assets (i.e. character names).
- No passwords are stored; nor credit card information is stored (payment is handled by Stripe.com).
- All data transmitted between client and server is under HTTPS.

4. XXE

- Not applicable as Pixton does not deal with XML; Pixton uses JSON to encode certain data.

5. Broken Access Control

- All Pixton API endpoints have appropriate access control in place (e.g. guest, user, admin-level).

6. Security misconfigurations

- Amazon Inspector (see https://aws.amazon.com/inspector/) reports no security misconfigurations or issues.

7. XSS

- All user-input data is escaped prior to storage, and prior to display.
- Pixton uses ReactJS for client-side UI rendering.

8. Insecure deserialization

- All user-input data is validated and sanitized prior to serialization.
- All serialization / deserialization is with JSON format.

9. Using components with known vulnerabilities

- All dependencies (i.e. Node packages) are periodically brought up to date.
- We only incorporate reputable, actively maintained and widely used Node packages into our codebase.

10. Insufficient logging and monitoring

- Key performance, exception frequency, and other metrics are monitored continuously using Amazon CloudWatch. Any anomalies can quickly be inspected and diagnosed.
- Pixton uptime is monitored continuously.

Results of Vulnerability Scans

API: https://api.pixton.com/*

No vulnerabilities founds.

API: https://render.pixton.com/*

No vulnerabilities founds.

What data does Pixton collect from teachers and/or students?

Category of Data	Elements	Description	Purpose
Application Metadata	IP address		Used to determine user's country of origin
	Use of cookies, local storage		Temporary storage of logged-in user session data
	Device type, OS, browser type and version		Used to determine whether browser supports the app
Application Use Statistics	Meta data on teacher interaction with application		May be analyzed to provide customer support to teachers, or to help improve product useability
Communications	Teacher comments to students		Allow teachers to provide written feedback to students within the app
Demographics	Gender	As selected by user during avatar creation	Gender selection influences what other options are available for the avatar (eg. outfits)
Enrollment	Student grade level	Specified by teacher when setting up a classroom	Used to set avatar age, and to customize messaging from app to teacher
Student Contact Information	Email address	Teacher chooses whether or not to submit students' email addresses	Used for single sign-on authentication only
Student Identifiers	Student app username	Teacher chooses whether or not to generate student usernames	Used for student authentication only
	Student app passwords	Teacher chooses whether or not to use a "login link" which acts, together with student usernames, as a proxy for student passwords	Used for student authentication only
Student Name	First and/or Last	Teacher chooses whether or not to submit students' real names	Used to identify user's avatar to other users within the same "classroom" group

			within the app
Student Work	Student generated content; writing, pictures, etc.	Student-generated avatar and comics	Student can select backgrounds, characters, outfits, poses, facial expressions to create comic panels; students can also freely input text into captions and speech / thought bubbles; student or their teacher can print, download, or share student comics via a link.
Teacher Contact Information	Email address		Used for single sign-on authentication only
Teacher Name	First and/or Last		Used to identify user's avatar and/or comments to student users within the same "classroom" group within the app
Teacher Work	Teacher generated content; writing, pictures, etc.		Teacher can select backgrounds, characters, outfits, poses, facial expressions to create comic panels; teachers can also freely input text into captions and speech / thought bubbles; teachers can print, download, or share their comics via a link.

What data does Pixton share with third parties, and which third parties?

Third Party	Data Shared	Purpose
Google Analytics	Teachers only; non-personal information only	Used in aggregate to track usage of the site; used to look up the usage history of a particular user, based on user SWID, for the purposes of customer support and useability analysis
Hubspot	Teacher email address and name; communications between teacher and Pixton	Used to provide customer support to teachers; solicit feedback from teachers; send Pixton-specific messages to teachers
Stripe	Teacher email address and name	Used to process credit card payments from teachers, and to manage paid subscriptions
Amazon Web Services	All account-related data; encrypted in transit and at rest	Used to host website and app, and to store all account-related data