

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Liverpool Central School District

and

Pixton Comics Inc.

This Data Privacy Agreement ("DPA") is by and between the Liverpool Central School District("EA"), an Educational Agency, and Pixton Comics Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor’s non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 2/5/2021 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New

York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Daniel Farsaci

Title: Director of Technology

Address: 190 Blackberry Road

City, State, Zip: Liverpool, NY 13090

Email: dfarsaci@liverpool.k12.ny.us

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.


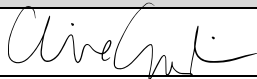
EDUCATIONAL AGENCY	PIXTON COMICS INC.
BY:	BY: 
Printed Name:	Clive Goodinson
Title:	CEO
Date:	Date: February 5, 2021

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: dfarsaci@liverpool.k12.ny.us. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

PIXTON COMICS INC.	
[Signature]	
[Printed Name]	Clive Goodinson
[Title]	CEO

Date:	February 5, 2021
--------------	-------------------------

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	See “Specific Third-Party Services” in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/
Description of the purpose(s) for which Contractor will receive/access PII	See “Specific Third-Party Services” in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date: ongoing Contract End Date: no defined end date
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: See attached document, Pixton Data Flow Diagram.pdf</p>
Encryption	Data will be encrypted while in motion and at rest.


CONTRACTOR	
[Signature]	
[Printed Name]	Clive Goodinson
[Title]	CEO
Date:	February 5, 2021

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See attached documents, Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Pixton Data Flow Diagram.pdf
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See Pixton Comics Security Policy.pdf
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	See Pixton Comics Security Policy.pdf
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See Privacy Policy at https://edu.pixton.com/educators/privacy-policy/
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Privacy Policy at https://edu.pixton.com/educators/privacy-policy/
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Privacy Policy at https://edu.pixton.com/educators/privacy-policy/
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See Privacy Policy at https://edu.pixton.com/educators/privacy-policy/

9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.
---	---	----------------------------

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor’s Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	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.	This degree of coordination is not necessary as we are a very small business (6 employees), and only one individual is assigned all security-related responsibilities.
	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.	This degree of coordination is not necessary as we are a very small business (6 employees), and only one individual is assigned all security-related responsibilities.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	This degree of coordination is not necessary as we are a very small business (6 employees), and only one individual is assigned all security-related responsibilities.
	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are	This degree of coordination is not necessary as we are a very small business (6 employees), and only one individual is assigned all security-related responsibilities.

	established and used to support operational risk decisions.	
	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.	N/A
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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	N/A
	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.	See Pixton Comics Security Policy.pdf and Pixton Data Flow Diagram.pdf
	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Anomalies are monitored through Amazon Web Services' CloudWatch, configured with alerts.
DETECT (DE)		

	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>Anomalies are monitored through Amazon Web Services' CloudWatch, configured with alerts.</p>
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>Anomalies are monitored through Amazon Web Services' CloudWatch, configured with alerts.</p>
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
RECOVER (RC)	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>
	<p>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).</p>	<p>See "Incident Response Plan" in Privacy Policy at https://edu.pixton.com/educators/privacy-policy/</p>

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