

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Pixton Comics Inc. ("Service Provider") on 10/31/2022 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.
Agree: Yes No
5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
Agree: Yes No
6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
Agree: Yes No
7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
Agree: Yes No
8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
Agree: Yes No
9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.
Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

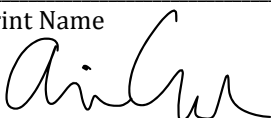
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Clive Goodinson

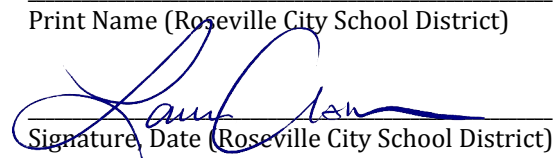
Print Name



Signature, Date

Laura Assem

Print Name (Roseville City School District)



Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

See attached:

Pixton Comics Security Policy v1.3.pdf

Pixton Data Flow Diagram.pdf

Section 1.7: Internal Security

See attached:

Pixton Comics Security Policy v1.3.pdf

Pixton Data Flow Diagram.pdf

Section II.2: Exporting of Student-Created Content

Please email privacy@pixton.com with a specific request.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Please email privacy@pixton.com with a specific request.

EXHIBITS

Section II.5: Securing Student Data

See attached:

Pixton Comics Security Policy v1.3.pdf

Pixton Data Flow Diagram.pdf

Pixton Data Collection - Teachers and Students.pdf

Section II.6: Disclosure Notification

Pixton Privacy policy Educator version.pdf

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See

https://ikeepsafe.org/content/uploads/2021/06/Please_DocuSign_iKeepProfile_FERPA_CSPC_COP_P-2.pdf

Section III.5: How Student Data is Protected:

See attached:

Pixton Comics Security Policy v1.3.pdf

Pixton Data Flow Diagram.pdf

Pixton Privacy policy Educator version.pdf

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 primarily with Amazon Web Services and HubSpot. 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.

Do not underestimate the costs associated with compromised data – our reputation, ability to succeed as a business, and the security of our users are at stake.

Alignment with NIST

This policy is intended to align with the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, from the National Institute of Standards and Technology (NIST 1.1) – see <https://www.nist.gov/cyberframework>.

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.

Pixton CMS – a private and proprietary, password-protected web app that designated Staff use for the purposes of creating and managing content, and assisting Pixton users.

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 educators, parents, business users, and solo users of Pixton, as well as many students, use Single Sign-on (SSO) to access their accounts. We do not store their passwords, even in an encrypted form. It would never be appropriate to ask for the user's password, such as for the purpose of accessing that user's Pixton account. Authorized Staff have an alternative, authenticated means of logging into a user's account for troubleshooting purposes, via the Pixton CMS.

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 the Pixton CMS;
- 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.

Some students, by the choice of their teacher, as well as all child and business client users, will access their accounts using a login link and a username. In this case, the login link and/or username can be considered to be the password, and Confidential. There should never be a reason to share or attempt to access login links or usernames, unless it's in order to support the associated educator / parent / business user's use of Pixton.

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 the Pixton CMS
- new features we're working on
- the Pixton product roadmap

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, eg. lesson ideas, content packs, background graphics, rubrics, 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 Privacy Officer.

Data Transmission and Storage

Users submit Confidential Information to us through various means:

- From the **Pixton web app**: data is stored securely with Amazon Web Services in Canada, encrypted in transmission and at rest using industry-standard algorithms so that it cannot be accessed by unauthorized parties. Most user data is submitted to Pixton this way.
- Through **HubSpot**: when certain types of users, including Educators, use Pixton, some of their information is automatically copied to Hubspot. This is for the purposes of customer support; analytics and product improvement; sales and marketing. When users use our Contact Us form or email support@pixton.com, the information they submit is also transmitted to and stored by Hubspot.
- Through **Typeform**: we occasionally administer surveys to Educators through this service. Any information submitted in this way is stored with Typeform.

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 reasonable 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://www.pixton.com/privacy-policy>). Otherwise, it is the responsibility of each Staff member to use their best judgment 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 computing device 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.

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 (ie. 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 Privacy Officer;
- If you suspect your password has been compromised in any way, you must change all potentially affected 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, unless permitted in writing by the Privacy Officer. 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.

Disciplinary Action

Anyone who fails to abide by this Policy may be subject to disciplinary action, which may include a retraining session with the Privacy Officer, or immediate termination for just cause.

If a breach of this Policy is suspected, access to user data and/or other systems by the employee or contractor in question, may be suspended while more information is gathered.

Incident Response Process and Procedures

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

If we ever discover or receive reports of a security breach, the Privacy Officer will:

1. Determine the severity of the potential impact. Is it real or perceived? Is it still in progress? What data is threatened and how critical is it? What is the impact on the business should the attack succeed – minimal, serious, or critical?
2. If the breach is real, determine the system(s) being targeted, along with all relevant details such as the attacker's IP address.
3. Determine how the incident can be contained, and contain it. This may involve changing passwords, encryption keys, or other system access information.
4. Determine what data has been compromised, and who should be notified about the incident.
5. Determine whether data has been lost and can/should be recovered, and how/when best to recover it.

6. Notify affected parties by email, no more than seven calendar days after discovery of the breach, including relevant details such as: the data that was compromised; the measures being taken to prevent any future such incidents.
7. Initiate data recovery, e.g. restoring the most recent automatic daily database backup.
8. Document the incident, including date detected, date occurred, notifications issued, and response.
9. Consider how the intrusion could have been prevented, and make changes to systems and/or policies accordingly.

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 unwittingly give up Protected 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 and a firewall on your devices, as well as password protection and automatic timeout to screensaver.

Onboarding and Decommissioning Devices

When acquiring a new laptop, mobile phone, or other electronic device used for work and which may ever store or process Protected Information, please provide the following information to the Privacy Officer (privacy@pixton.com):

- Device – eg. laptop; phone
- Type – eg. MacBook Pro; iPhone XR
- OS including version – eg. macOS v12.31; iOS v15.3.1
- Drive encryption status – ON or OFF
- Firewall status – ON or OFF
- Anti-virus status – ON or OFF
- Screen lock type – eg. password; fingerprint; FaceID
- Owner – Pixton; you
- Apps containing Protected Information – eg. HubSpot; Slack; Pixton CMS
- Date acquired

When replacing, upgrading, or decommissioning laptops, mobile phones, or other electronic devices used for work that have ever contained or processed Protected Information, it's crucial to ensure that the Protected Information is no longer accessible. First, communicate to the Privacy Officer (privacy@pixton.com) in an email, details about the device to be decommissioned. The Privacy Officer will instruct you what to do with the device. You may be instructed to perform a complete system reset and operating system reinstallation on the device.

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. Vulnerability scans can be performed through code review, or via vulnerability scanning software such as Wapiti (see <https://github.com/wapiti-scanner/wapiti>).

Results of Vulnerability Scans, July 2021

The Pixton web app and RESTful API were last reviewed in April 2022, using the Wapiti web vulnerability scanning program. No major issues were found, and several minor issues were promptly addressed. Some minor issues are known and remain, due to the limitations of certain dependencies. Results are available by request from the Privacy Officer.

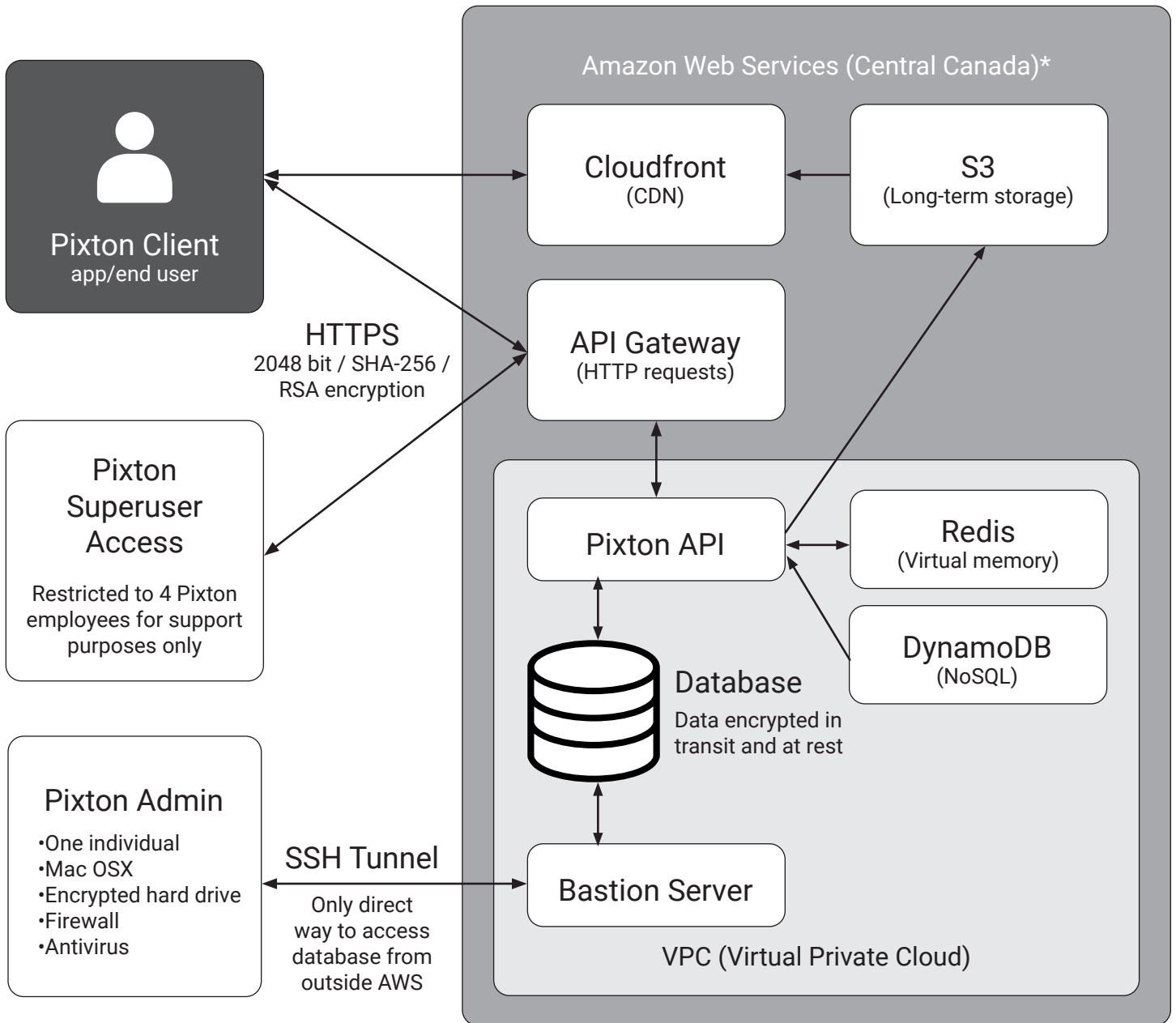
Category of Data	Elements	Description	Purpose
Application Metadata	IP address		Used to determine user's country of origin
	Use of cookies, local storage		Temporary storage of logged-in user session data
	Device type, OS, browser type and version		Used to determine whether browser supports the app
Application Use Statistics	Meta data on teacher interaction with application		May be analyzed to provide customer support to teachers, or to help improve product useability
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.com	Teachers only; 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.com	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; data stored in Canada

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.

Privacy Policy – Educator / Student version

Last Update: August, 2021

Introduction and Definitions

Pixton Comics Inc. (“PCI”) is committed to maintaining the security, confidentiality and privacy of your Personal Information (which includes the Personal Information of Students).

This privacy policy (the “Privacy Policy”) constitutes an agreement between you, or if you are under the age of majority in your local jurisdiction, you, with the consent of your parent or legal guardian, (“user”, “you” or “your”) and PCI and its affiliates and subsidiaries (collectively, “Pixton”, “us”, “our” or “we”). Pixton is dedicated to protecting the privacy rights of our users. This Privacy Policy describes how Pixton collects, protects, uses, retains, discloses, purges and destroys information and data created in the course of your access to and use of the Site, Content and/or Services (each as defined below). Please note that this Privacy Policy applies only to information collected through the Site and/or Services.

We have designated a Privacy Officer who is responsible for this Privacy Policy. The Privacy Officer's contact information is as follows:

Name: Clive Goodinson

Address: c/o Pixton Comics Inc., PO Box 123, Qualicum Beach, BC, Canada V9K 1S7

Phone: 1 (888) 774-9866

Email: privacy@pixton.com (<mailto:privacy@pixton.com>)

For the purposes of this Privacy Policy:

“Child or Children” means any child or children under the age of 13 years old.

“Content” means any expression fixed in a tangible medium and includes, without limitation, ideas, text, graphics, avatars, designs, presets (including but not limited to: backgrounds, scene configurations, characters, outfits, body poses, facial expressions, color filters, overlays, effects), combinations of presets, drawings, logos, images, trademarks, copyrights, information, software, and any intellectual property therein, any of which may be created, submitted, or otherwise made accessible on or through the Site and/or Services.

“Educator(s)” means a teacher or individual employed by an educational institution, or the educational institution itself.

“Pixton Content” means all Content that is not User Generated Content.

“Services” means creation of avatars, characters and scenes with accompanying text for a comic strip accessed through the Site, as well as access to preset Content including but not limited to: backgrounds, scene configurations, characters, outfits, body poses, facial expressions, color filters, overlays and effects.

“Site” means www.pixton.com, app.pixton.com, and other affiliated subdomains of pixton.com.

“Student” means a student who enrolls in a Student Sub-Account upon an Educator's provision of a registration code or link.

“User Generated Content” or “UGC” means any material whatsoever, including comics, that a user, including you, submits, creates, transfers or otherwise makes available by access to the Site or through the Services, including but not limited to ideas, information, images, data, text, graphics, designs, drawings or other Content posted in any area within the Site or through the Services.

Compliance with Privacy Laws

Pixton is compliant with the requirements of Canadian and US privacy laws including:

- **United States:** the Children’s Online Privacy Protection Act (“COPPA”); the Family Educational Rights and Privacy Act (“FERPA”)
- **California:** the California Consumer Privacy Act (“CCPA”); the Student Online Personal Information Protection Act (“SOPIPA”)
- **Illinois:** the Student Online Personal Protection Act (“SOPPA”)
- **New York:** Education Law Section 2-D (“Ed 2d”)
- **Washington:** the Student User Privacy in Education Rights (“SUPER”) Act
- **Canada:** the Personal Information Protection and Electronic Documents Act (“PIPEDA”)
- **Alberta:** the Freedom of Information and Protection of Privacy Act (“FOIP”)
- **British Columbia:** the Personal Information Protection Act (“PIPA”)
- **Ontario:** the Municipal Freedom of Information and Protection of Privacy Act (“MFIPPA”)

Don't hesitate to contact privacy@pixton.com if you are unsure whether Pixton complies with your local privacy laws – chances are, we do!

Pixton Comics participates in the iKeepSafe Safe Harbor program. If you reside in the United States and have any questions or need to file a complaint related to our privacy policy and practices, please do not hesitate to contact the iKeepSafe Safe Harbor program at COPPAprivacy@ikeepSAFE.org (<mailto:COPPAprivacy@ikeepSAFE.org>).

Acceptance of Terms and Revisions

In order to use the Services, COPPA requires verifiable parental consent to the use, collection and disclosure of their Child's personal information. COPPA allows Educators to act in the place of parents or guardians to provide consent to the collection of personal information from Children. If the Services are employed in a school setting, Pixton requires Educators to consent to Pixton's [Terms of Use](https://www.pixton.com/terms-of-use/educators) (<https://www.pixton.com/terms-of-use/educators>) and this Privacy Policy prior to the collection of personal information about a Child. For your convenience, we provide a [parental consent letter](https://docs.pixton.com/edu/pixton-parental-consent-letter.pdf) (<https://docs.pixton.com/edu/pixton-parental-consent-letter.pdf>) for schools to use as they see fit.

If consent of an Educator is not required in your jurisdiction, then by accessing the Site, submitting information to us (regardless of whether you register an Account or Student Sub-Account with us) or downloading, installing or using any of the Content or Services you accept the terms of this Privacy Policy. If you do not accept the terms of this Privacy Policy you must not submit information to or register an account with us, access the Site or download, install or use any of the Content or Services.

We reserve the right to revise this Privacy Policy at any time. We will give you notice of such revisions by posting the revised Privacy Policy at <https://www.pixton.com/privacy-policy/educators> (<https://www.pixton.com/privacy-policy/educators>) and by posting a popup notification when you next log in, containing a link to the latest Privacy Policy as well as an "I Agree" button that you must click in order to accept those revisions and continue using the Site and/or Services. If we make a material change to this Privacy Policy which affects the types of personal information that we collect from Children or Educators we shall notify Educators by email of such changes to this Privacy Policy, no fewer than 30 days before said changes are put into effect. If additional verifiable consent is required by law when changing the Privacy Policy, Pixton requires a Child's Parent to provide consent to such amendments and provide consent on behalf of any Child prior to the collection, use or disclosure of any personal information not previously consented to.

Types of Information We Collect

There are two types of information we may collect through your access to and use of the Site and/or Services:

- a. "Personal Information" means information about an identifiable individual (including any "Personal Information" as such term is defined in the applicable privacy statute). Personal Information may include for example, but is not limited to, a person's first and last name, an email address, a user name, persistent identifiers such as IP address or device number, a photograph, or any anonymous information combined with a persistent identifier or other Personal Information.
- b. "Non-Personal Information" means information that does not identify you and cannot be used to identify you personally and may include your browser and operating system descriptor, date of birth, age, gender, and non-precise geolocation information (e.g., your city). For Student users Non-Personal Information includes your grade level and subject area if this information is made anonymous and de-identified. Non-Personal Information also includes "Usage Data" which is anonymous data associated with your computer that includes activities and time on the Site, when not linked to any persistent identifier or other Personal Information.

No Personal Information is necessarily needed by Pixton for the registration of any Student Sub-Accounts. If you select the Username method of Student authentication for your classroom, you may input a pseudonym for each Student instead of each Student's real name.

Application of this Privacy Policy

This Privacy Policy only applies to the information that Pixton collects and uses, or is supplied, through the access to and use of the Site and/or Services. Any information disclosed to any third party is dealt with in accordance with the privacy policies adopted by each of those third parties. We do, however, only use third party services whose policies are consistent with our own. We encourage you to review the privacy policies maintained by each of those third parties to understand how their information will be used by those entities to process requests. For example, we partner with third party service providers and vendors to provide access to existing payment gateways and your credit card, banking and other billing information is kept with our payment processor, Stripe, and you can read about its privacy policy at the following link:

<https://www.stripe.com/privacy-center/legal>

(<https://www.stripe.com/privacy-center/legal>). In the case that COPPA applies in your jurisdiction, then parents, guardians, or Educators in place of them, have a choice to consent to the disclosure of their Child's personal information to third parties unless such disclosure is integral to the Services.

Collection of Information

We may collect information (including Personal Information) as follows:

- a. **Information you provide to us upon registration.** If you choose to register, complete a sign-up form or group register form, open an account or become a member with us, request support, or in any other way take steps that require the submission of information, we may collect Personal Information such as your email address, and for Educators only, your name.
- b. **Purchases.** If you choose to subscribe to the Site and/or Services, our payment processor, Stripe, will collect your credit card information. We do not collect or store your credit card information.
- c. **Information you submit to us.** If you choose to submit your information to us for any other reason in any other form, we will collect such information and use it for the purposes for which you submitted it. In COPPA applicable jurisdictions, you will need to submit verifiable parental, guardian or Educator consent prior to submitting personal information if not previously consented to.
- d. **Visiting our Site.** We will not collect any Personal Information from you simply by virtue of your visiting the Site; we only collect Personal Information if you choose to submit it to us. We do, however, collect Non-Personal Information such as Usage Data, whenever you use the Site and/or Services. If prohibited in your jurisdiction, such Non-Personal Information is not combined with Personal Information.
- e. **Where permitted by law.** We may also collect information, including Personal Information as otherwise permitted by law.
- f. **Browser privacy preference.** We will use reasonable efforts to comply with the privacy preference setting in any browser, but generally do not comply with any Do-Not-Track requests on browsers.
- g. **Email messages.** We may collect Non-Personal Information through emails we send you which contain code that allows us to track whether the message was opened and/or links were clicked.
- h. **Cookies.** In connection with the foregoing collection of information, we may also use “cookies” or similar technologies (small amounts of data that are stored on your computer's hard drive when you use or access the Site and/or Services that identify your computer and may store information about you such as behavioural data). Should you choose to submit Personal Information to us, we may link cookie information to such Personal Information. If you do not wish to accept cookies, you have the option of blocking or disabling cookies. However, please be aware that some of the Site and/or Services will not function properly if you do so and you may lose access to Services you purchased. In light of the above, if you happen to be

in a jurisdiction in which COPPA applies, we will not collect any Personal Information with cookies and will not link any cookie information with Personal Information without verifiable parental consent.

- i. **Third party advertisers.** No third-party advertising is permitted on the Site.
- j. **User-generated content.** All users can enter comic titles, speech / thought bubble text, and captions with no restrictions other than length. All users can create an avatar, which may or may not be an accurate representation of themselves in real life. Users attached to all-access subscriptions can upload images into the backgrounds of their comic panels.

We strongly advise you not to submit Personal Information as part of UGC, comics or other content you create. However, if you do, the Personal Information will be stored in our database and treated the same as other Personal Information collected from you.

Public Disclosure of User Generated Content and Other Internet Activity

By default, all UGC attached to a Student Sub-Account is visible only to that student, and to their Educator.

You or your Student Sub-Account holder may choose to disclose information about yourself in the course of creating User Generated Content to us or through your use of the Site and/or Services. You may generate a "Share Link" on the Site for any of your own comics, and for any of your Student Sub-Accounts. Students may also generate a Share Link for any of their own comics. Note that Share Links generated for comics created by Children redirect to a login page such that only an authorized Educator can view the shared comic (i.e., the comic cannot be shared publicly). Otherwise, comics viewable via a Share Link never include the Student's name or username. However, the comic title and any text in the comic are displayed unchanged. Both the Student and the Educator have the ability to edit a comic and remove any Personal Information from it, before sharing it.

We are not responsible for the Personal Information you choose to make public through a Share Link, or through printing or downloading copies of UGC outside of the Site. Please see our Terms of Use at <https://www.pixton.com/terms-of-use/educators> (<https://www.pixton.com/terms-of-use/educators>) for other guidelines about sharing content on the Site.

Use of Your Information

We may use your information (including Personal Information) for the following purposes:

- a. to provide you with any services or functionality you have requested, including the Services;
- b. to improve the Site and/or Services, and to inform the creation of future Services;
- c. to send you information related to the Site and/or Services, including confirmations, Site news, technical notices, updates, security alerts, and support and administrative messages;
- d. to process transactions for the Services;
- e. to manage your account with Pixton;
- f. to respond to customer service inquiries;
- g. to troubleshoot problems with the Site and/or Services;
- h. to enforce our Terms of Use (available at <https://www.pixton.com/terms-of-use/educators> (<https://www.pixton.com/terms-of-use/educators>));
- i. to protect against unlawful activities or other misuse of the Site and/or Services or for other security reasons;
- j. to compile statistics;
- k. for Educators only, to invite you to participate in Pixton surveys, contests or special events;
- l. to allow you to share your User Generated Content with your colleagues, friends or family;
- m. to authenticate your identity; and
- n. to integrate third-party authentication, including Google or Microsoft single sign-on.

By providing Personal Information through the access to, or use of, the Site and any of the Services, you acknowledge, consent and agree that we may use the Personal Information for the purposes set out in this Privacy Policy and by accessing, using, or installing any of the Site and/or Services or submitting information to us you also agree that we may use the Non-Personal Information for the purposes set out in this Privacy Policy. To be clear, we will never use Student information for any commercial purposes whatsoever.

Specific Third-Party Services

The Site makes use of the following third party services:

- a. Google Analytics (Educators only) collects Non-Personal Information, which we use aggregated and anonymized to track the usage of the Site. No User Generated Content is passed to Google Analytics.
- b. Hubspot.com (Educators only) is a customer communication tool that allows us to send email and in-application messages to Educators. We use it to segment Educators for more specific messaging; to organize messages; and to communicate product updates such as feature releases. This service collects limited Personal Information, such as name and email address.
- c. Stripe.com (Educators only) is a payment processor, which we use to collect credit card payments from Educators. This service collects limited Personal Information, such as name and credit card information.
- d. Google, Microsoft, or Facebook (Educators only) facilitate single sign-on to the Site. We use them to authenticate users and to retrieve the name and/or email address of the user, for the purposes of provisioning and then enabling access to a Pixton account. These services collect and pass to Pixton limited Personal Information (name and email address).
- e. Amazon Web Services is a set of cloud-based web hosting services. We use it to host the Site, including the database where user data are stored. This service does not collect Personal Information, although it may store (in an encrypted format) such data as collected and stored by Pixton.

FERPA and California AB 1584

Consistent with FERPA and California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1), PCI will abide to the following for all users:

- a. Student records obtained by PCI from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights to the personal information and education records it provides to PCI.
- b. PCI users may retain possession and control of their own User Generated Content.
- c. PCI will not use any information in a student record for any purpose other than those required or specifically permitted by Pixton's [Terms of Use](https://www.pixton.com/terms-of-use/educators) (<https://www.pixton.com/terms-of-use/educators>) and this Privacy Policy.
- d. Parents, legal guardians, or eligible students may review personally identifiable information in the student's records and correct erroneous information by contacting their educational institution. Additionally, Users

may access, correct, update, or delete personal information in their profile by signing into the Site, accessing their account, and making the appropriate changes.

- e. PCI is committed to maintaining the security and confidentiality of student records. Towards this end, we take the following actions: (a) we limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities; (b) we conduct background checks on our employees that may have access to student data; (c) we conduct regular employee privacy and data security training and education; and (e) we protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.
- f. In the event of an unauthorized disclosure of a student's records, PCI will promptly notify Users unless specifically directed not to provide such notification by law enforcement officials. Notification shall identify: (i) the date and nature of the unauthorized use or disclosure; (ii) the Personal Information used or disclosed; (iii) general description of what occurred including who made the unauthorized use or received the unauthorized disclosure; (iv) what PCI has done or shall do to mitigate any effect of the unauthorized use or disclosure; (v) what corrective action PCI has taken or shall take to prevent future similar unauthorized use or disclosure; and (vi) who at PCI the User can contact. PCI will keep the User fully informed until the incident is resolved.
- g. PCI will delete or de-identify personal information when it is no longer needed, upon expiration or termination of our agreement with an educational institution with any deletion or de-identification to be completed according to the terms of our agreement with the educational institution, or at the direction or request of the educational institution.
- h. PCI agrees to work with educational institution to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described in statement (4) above.
- i. PCI prohibits using personally identifiable information in student records to engage in targeted advertising.

Disclosure of Information

We will not transfer your Personal Information to third parties beyond the specific third party services listed above. Notwithstanding the foregoing, we reserve the right to disclose information, including Personal Information, if we reasonably believe that we are required to do so by law or legal process or if we are

otherwise requested by any law enforcement officer or agency acting under colour of law. In addition, we reserve the right to disclose Personal Information and Non-Personal Information in order to (a) enforce the Terms of Use (available at <https://www.pixton.com/terms-of-use/educators> (<https://www.pixton.com/terms-of-use/educators>)); (b) investigate and/or take action against unlawful activity, suspected abuse or unauthorised use of the Site and Services; (c) protect and defend the rights or property of Pixton; or (d) act in urgent circumstances to protect the safety or security of the public or users of the Site and Services. We may also disclose your information (including Personal Information) in connection with a corporate re-organization, a merger or amalgamation with another entity, or a sale of all or a substantial portion of our assets provided that the information disclosed continues to be used for the purposes permitted by this Privacy Policy by the entity acquiring the information. In the event of a merger, amalgamation, or sale, we will provide you notice by email no fewer than 30 days in advance of said event. We will take all steps necessary to inform all users of all data collection conducted by legal authorities through all legal channels.

Protection of Your Information

Pixton has implemented reasonable physical and technical measures to protect the information we collect or are provided with from unauthorized access and against loss, misuse or alteration by third parties, including but not limited to:

- Containment of database(s) inside a Virtual Private Cloud (VPC), access to which is extremely restricted;
- Encryption of database data in transit and at rest;
- Use of SSL / HTTPS for all data transmission over the Internet;
- Multifactor authentication on administrator-level access;
- Code reviews and scans to monitor for security vulnerabilities;
- Firewalls, private keys, anti-virus protection, IP address whitelists, and encrypted local hard drives.

Further, while we attempt to ensure the integrity and security of our network and systems, we cannot guarantee that our security measures will prevent third-party "hackers" from illegally obtaining access to this information. We do not warrant or represent that your information will be protected against, loss, misuse, or alteration by third parties. No method of transmission over the Internet, or method of electronic storage, is 100% secure.

PIXTON STRIVES TO EXCEED COMMERCIALY REASONABLE EFFORTS TO PROTECT YOUR PERSONAL INFORMATION, HOWEVER, TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE EXPRESSLY DISCLAIM ANY GUARANTEE OF SECURITY IN CONNECTION WITH

YOUR PERSONAL INFORMATION.

For further information on how we safeguard information we collect or are provided with, contact us via email at privacy@pixton.com.

Incident Response Plan

If we ever discover or receive reports of a security breach, we will take the following steps to address it:

- The staff member who detects or receives a report of a breach will forward all details to Pixton's privacy officer at privacy@pixton.com.
- The privacy officer will:
 1. Determine the severity of the potential impact. Is it real or perceived? Is it still in progress? What data is threatened and how critical is it? What is the impact on the business should the attack succeed – minimal, serious, or critical?
 2. If the breach is real, determine the system(s) being targeted, along with all relevant details such as the attacker's IP address.
 3. Determine how the incident can be contained, and contain it. This may involve changing passwords, encryption keys, or other system access information.
 4. Determine what data has been compromised, and who should be notified about the incident.
 5. Notify affected parties by email no more than seven calendar days after the discovering of the breach, including relevant details such as: the data that was compromised; the measures being taken to prevent any future such incidents.
 6. Document the incident, including date detected, date occurred, notifications issued, and response.
 7. Consider how the intrusion could have been prevented, and make changes to systems and/or policies accordingly.

Retention of Your Information

The data and information that we collect will be stored and maintained by Pixton or our third-party service providers until you delete it or instruct us to delete it, or until your Account is terminated by us. We will retain data and information we collect for a period of 60 days after your Account is terminated, at which time it will be permanently deleted. We intend to only retain data, including Dependent data, for as long as is reasonably necessary to fulfill the purpose for which the

information was collected. Any Student account belonging to a deleted group, and to no active or archived groups, will be permanently deleted 60 days after you flag the group for deletion.

To request deletion of your account or deletion of a Student's account, please email our Privacy Office at privacy@pixton.com (<mailto:privacy@pixton.com>) with specific details, such as the email address or username on the account and the date you wish it to be deleted. In order to verify your identity and authorization to make a deletion request, we will only correspond using the email address associated with your Educator Account.

Currently, Pixton or our third party service providers retain and store information collected by, or provided to, us in the cloud and on secure servers in Canada. You hereby consent to Pixton storing any Personal Information you provide to us on secure servers in Canada.

Account Security

If you access the Site and/or use any of the Services, you are responsible for protecting the confidentiality of your account password and elected codes, and for restricting access to your computer and you agree to accept responsibility for all activities that occur under your account. Please notify us immediately if you detect suspected misuse of your account via email at: privacy@pixton.com.

Access and Accuracy

Pixton will use commercially reasonable efforts to provide you access to your Personal Information (to the extent we are in possession of any) if you submit your request for access via privacy@pixton.com. Pixton may charge you a reasonable fee for doing so. Students who wish to access their Personal Information must have the Educator submit a request on their behalf. Subject to applicable law, including COPPA, Pixton reserves the right to deny access to your Personal Information on any of the following grounds:

- a. when denial of access is required by law;
- b. when granting you access is reasonably likely to negatively impact other people's privacy;
- c. when granting access is, in our judgement and acting reasonably, cost prohibitive; or
- d. when we have reason to believe that such requests are frivolous or made in bad faith.

You are responsible for ensuring that all information created through your access to and use of the Site and/or Services is accurate, reliable and complete and you acknowledge and accept that the use of such information is at your

own risk. We can only provide accurate Services if we are in possession of your current and accurate information, therefore, we ask that you keep any Personal Information that you provide to us current and accurate. You represent and warrant that all Personal Information you provide us is true and accurate and relates to you and not to any other person. If you believe that the Personal Information maintained by Pixton about you is inaccurate or incomplete, you may notify us by describing in detail any inaccuracies or omissions via email at privacy@pixton.com. Following receipt of a properly submitted notice, we will, within a reasonable time period and acting in our sole discretion, use commercially reasonable efforts to either: (a) amend or correct your Personal Information to reflect corrected or additional information provided by you, or (b) in connection with your Personal Information, make note of any claimed inaccuracies or omissions reported in the notice submitted by you.

Our Policy Regarding Children

Pixton recognizes the privacy interest of children and we encourage parents/guardians to take an active role in their children's use of the Site and/or Services. Children under the age of majority in their local jurisdiction may only use the Site and/or Services through the use of a sub-account (a "Student Sub-Account") linked to an Educator's account. If an Educator wishes for a Student under the age of majority in their local jurisdiction (each a "Permitted Minor"), to use the Site and/or Services, after obtaining consent from the Permitted Minor's parent or legal guardian, the Educator may provide either (a) a "Join Link" to the Permitted Minor so the Permitted Minor can self-register a Student Sub-Account using the Single Sign-on method chosen by the Educator, or (b) a "Login Link" and Username to the Permitted Minor so the Permitted Minor can access their Student Sub-Account. Student Sub-Accounts may only be opened, accessed, modified or deleted through the Educator's account. ANY EDUCATOR WHO PRESENTS A REGISTRATION CODE OR LINK TO A PERMITTED MINOR FOR A PERMITTED MINOR TO REGISTER A STUDENT SUB-ACCOUNT LINKED TO THE EDUCATOR'S ACCOUNT HEREBY REPRESENTS AND WARRANTS THAT THE EDUCATOR HAS OBTAINED THE NECESSARY CONSENTS FROM THE PARENT OR LEGAL GUARDIAN OF EACH PERMITTED MINOR AS REQUIRED UNDER THIS PRIVACY POLICY.

Upon a Student registering a Student Sub-Account, the Educator may access, modify or delete the Students' information and UGC by:

- a. selecting the areas of the Site and information, including text, images, data or other Content posted on the Site and/or available through the Services, that the Student may access through the Student Sub-Account; and
- b. viewing the Student Sub-Account users' recent activity, including UGC created by the Student.

If Pixton discovers, or if a parent/guardian or Educator becomes aware, that a Student under the age of majority in their local jurisdiction has accessed the Site and/or Services on their own and without the use of a Student Sub-Account, or provided us with information without the parent/guardian's consent, please contact us at privacy@pixton.com. We will delete such information from our files within a reasonable time.

If you are below the age of majority in your local jurisdiction, please obtain your parent's, legal guardian's, or Educator's permission before accessing or using any of the Site and/or Services or providing us with any Personal Information or Non-Personal Information.

In the interests of the safety and comfort of all users under the age of majority in your local jurisdiction, we reserve the right, acting in our sole discretion but without any obligation, to restrict the access of any user to any space on the Site.

Educator Moderation

Educators can see all User Generated Content created by Students within their group(s), whether completed or in progress. The Educator has the ability to delete User Generated Content created by Students within their group(s). User Generated Content may be shared online through the Share Link – publicly if the student is not a Child – and shared publicly offline through printing hard copies of User Generated Content. THE EDUCATOR IS RESPONSIBLE FOR PROTECTING AGAINST THE DISCLOSURE OF ANY PERSONAL INFORMATION AND WHICH IS INCLUDED IN USER GENERATED CONTENT AND SHARED EITHER PUBLICLY ONLINE OR OFFLINE. TO THE EXTENT ALLOWABLE BY LAW, PIXTON DISCLAIMS ALL RESPONSIBILITY AND LIABILITY AND THE EDUCATOR HEREBY ACKNOWLEDGES AND ACCEPTS ALL RESPONSIBILITY AND LIABILITY FOR ANY DISCLOSURE OF PERSONAL INFORMATION THROUGH USER GENERATED CONTENT, INCLUDING THROUGH THE ONLINE "SHARE LINK" OR OFFLINE THROUGH PRINTING THE USER GENERATED CONTENT.

Governing Law

Those who choose to use or access the Site and/or Services from outside Canada do so on their own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable. Pixton is compliant with US privacy laws, as listed above, but does not make the same claim for all countries outside Canada. Notwithstanding the foregoing, and recognizing the global nature of the Internet, each viewer and user shall comply with all local rules regarding online conduct and creation of acceptable materials. This Privacy Policy and your legal relationship with Pixton shall be governed by, and will be enforced, construed, and interpreted in accordance with the laws of the province of British Columbia, Canada and the federal laws of Canada applicable therein, without regard to principles of conflicts of law. All disputes between you and Pixton will be resolved by, and you hereby submit to, the exclusive jurisdiction of the courts of British Columbia in Vancouver.

International Transfer

We may transfer information that we collect about you to third parties across borders and from your country or jurisdiction to other countries or jurisdictions around the world. Please note that these countries and jurisdictions may not have the same personal information protection laws as your own jurisdiction, and you consent to the transfer of information over international borders and the use and disclosure of information about you, including Personal Information, as described in this Privacy Policy. We or our third party service providers store your Personal Information in Canada.

Questions or Comments

We welcome questions or comments about this Privacy Policy. Please direct any questions or comments to the individual below who oversees Pixton's compliance with privacy requirements:

Pixton Comics Inc.

Attention: Privacy Officer

Email: privacy@pixton.com