RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Clever Prototypes, LLC (DBA Storyboard That) ("Service Provider") on 3/22/2022 ("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 ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

Aaron Sherman, CEO
Print Name

DocuSigned by:
Aaron Sherman
40952C4C3532484...
3/22/2022
Signature, Date

Laura Assem, 3/22/2022
Print Name (Roseville City School District)

Laura Assem
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security
Please see attached documents

Section 1.7: Internal Security
Please see attached documents

Section II.2: Exporting of Student-Created Content
Please see attached documents

Section II.4: Review and Correcting Personally Identifiable Information (PII)
Please see attached documents

EXHIBITS

Section II.5: Securing Student Data

Please see attached documents

Section II.6: Disclosure Notification

Please see attached documents

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

Please see attached documents

Section III.5: How Student Data is Protected:

Please see attached documents

intruder

Scan Summary: **Aaron Sherman**

Targets: **api.storyboardthat.com, backend.storyboardthat.com, www.storyboardthat.com, www.test.storyboardthat.com**

17 March 2022

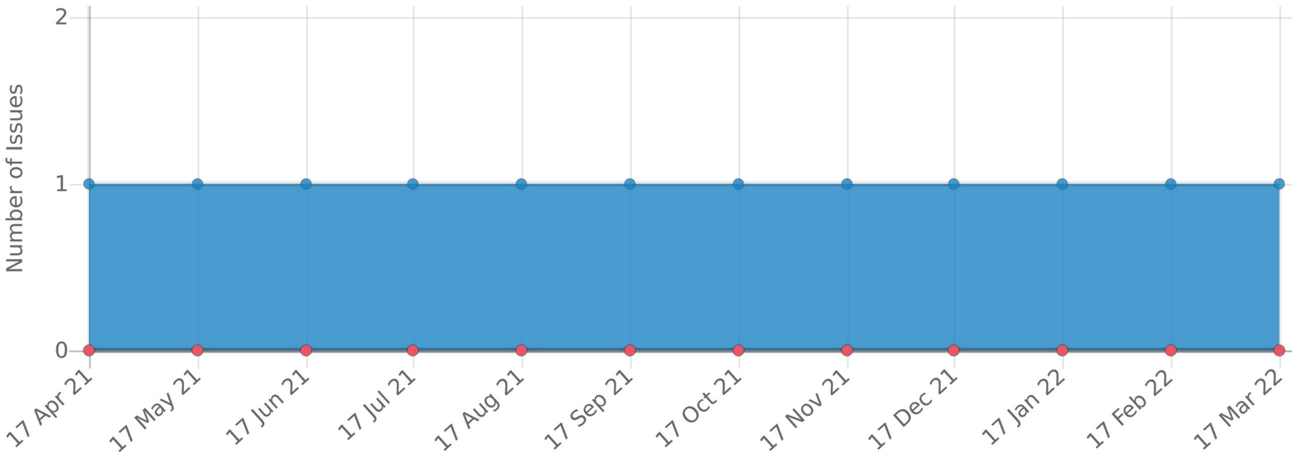
Low

Threat Level

Low severity issues can not directly be exploited by an attacker, but may increase the ease of exploiting more severe issues in future. Fixing these issues may help protect against weaknesses that are not publicly known, or be used as one component in a highly targeted attack by the most sophisticated and well resourced attackers.

0	0	0	1
Critical issues	**High** issues	**Medium** issues	**Low** issues

Exposure over time



Differences since last assessment

New issues discovered		Previous issues remediated		Direction of travel
Critical	0	Critical	0	▯ 0
High	0	High	0	▯ 0
Medium	0	Medium	0	▯ 0
Low	0	Low	0	▯ 0

What we checked

Total checks
11,057

Targets
4

Issues discovered
1

Here are some examples of what we checked your targets and their reachable webpages for.

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

As a **Pro** plan customer, you also have access to:

Emerging threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organizations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check.

Internal checks

Your internal systems can also be hacked with a little extra effort, e.g. by an email or web page link that exploits known unpatched software or an employee's device. Our agent-based scanner can be installed on each machine you want to protect.

Issue Summary

Severity	Issue details
Low	**Strict Transport Security HTTP Header Not Set** Number of occurrences: 2

Issues

Strict Transport Security HTTP Header Not Set (Low)

Description

The server does not set a “Strict Transport Security” HTTP header in its response.

The HTTP Strict Transport Security policy defines a timeframe within which a browser must connect to the web server via HTTPS. The header adds additional protection against MitM (Man-in-the-Middle) attacks by instructing the user's web browser not to connect to the server unless it is done so over HTTPS with a valid certificate. This helps prevent an attacker in a MitM position from tricking the user into connecting to an attacker controlled server which is impersonating the targeted site.

Remediation Advice

Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]

The parameter max-age gives the time frame for requirement of HTTPS in seconds and is recommended to be set for at least several months, with 90 days being a minimum (ie. 7776000 seconds). The flag includeSubDomains defines that the policy should also apply for sub domains of the sender of the response.

For example, the following lines can be added to an Apache configuration file:

```
Header set Strict-Transport-Security "max-age=7776000"
Header append Strict-Transport-Security includeSubDomains
```

Occurrences

	First seen
api.storyboardthat.com : 443 (tcp)	18 Sep 2020 22:25
backend.storyboardthat.com : 443 (tcp)	18 Sep 2020 21:27

Snoozed

The following issue occurrences are currently snoozed.

Issue	Occurrence	Reason	Details	Snoozed until
Untrusted TLS Certificate	www.storyboardthat.com : 8172 (tcp)	False positive	we believe port 8172 is a control port thats used by azure	Forever
Untrusted TLS Certificate	api.storyboardthat.com : 8172 (tcp)	False positive	we believe port 8172 is a control port thats used by azure	Forever
Untrusted TLS Certificate	www.test.storyboardthat.com : 8172 (tcp)	False positive	we believe port 8172 is a control port thats used by azure	Forever

Raw Reconnaissance Data

Target (IP and Hostnames)	Port	Protocol	Service	Service info
137.117.56.115 backend.storyboardthat.com	80	tcp	http	Microsoft IIS httpd 10.0
	443	tcp	ssl	Microsoft SChannel TLS
104.45.152.60 www.storyboardthat.com	443, 454 - 455, 8172	tcp	ssl	Microsoft SChannel TLS
40.71.0.179 api.storyboardthat.com	4024	tcp	tnp1-port	
	1221	tcp	http	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
	4022	tcp	dnox	
104.45.152.60 www.storyboardthat.com	7654	tcp	unknown	
40.71.0.179 api.storyboardthat.com	80	tcp	http	Microsoft IIS httpd 10.0
	443, 454 - 455, 8172	tcp	ssl	Microsoft SChannel TLS
104.45.152.60 www.storyboardthat.com	1221	tcp	http	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
	4022	tcp	dnox	
40.71.0.179 api.storyboardthat.com	7654	tcp	unknown	
104.45.152.60 www.storyboardthat.com	4024	tcp	tnp1-port	
	80	tcp	http	Microsoft IIS httpd 10.0

Scan Info

Targets included in this scan

api.storyboardthat.com
www.storyboardthat.com
backend.storyboardthat.com
www.test.storyboardthat.com

Scan timings

This scan ran from 17 Mar 2022 00:05 to 17 Mar 2022 15:34.

About us

intruder

Company

Intruder Systems Ltd is an independent security advisory company, specialising in providing continuous security monitoring for internet-facing web applications and infrastructure.

Credentials

Intruder is a member of CREST

Intruder is a CREST accredited Vulnerability Assessment service

Monitored by Drata for SOC 2 compliance

National Cyber Security Centre CiSP

Intruder is a member of the Cyber-security Information Sharing Partnership

CYBER ESSENTIALS

Intruder is Cyber Essentials certified.

GCHQ Cyber Accelerator Alumni

Security Team

Our consultants have delivered work for government agencies, international financial institutions, and global retail giants.

Compliance

Our reports are ISO 27001 and SOC 2 compliance ready.

Contact

 contact@intruder.io

 www.intruder.io

 twitter.com/intruder_io

 linkedin.com/company/intruder

Student Privacy and Storyboard That

storyboardthat.com/about/privacy-for-schools

This is an addendum to our Terms of Use and Privacy Policy that only apply for our educational edition. Learn about our educational edition.

We are constantly looking to improve our policies. Please contact us at Contact-Us@StoryboardThat.com if you feel we need further clarification, or are missing something.

Although no system is 100% perfect, we have designed our system and taken reasonable precautions and then some to follow these policies to address concerns of **FERPA**, **CCPA**, **GDPR**, and **COPPA**. We have also signed the Student Privacy Pledge.

Our Business Model

Our business model in the education space is to provide an amazing product leveraging the power of digital storytelling to positively improve Critical Thinking, Communication, Collaboration, and Creativity. We sell this product directly to teachers and schools, and all of our marketing efforts are centered on this objective.

We do not market to kids and students, since they are not a target purchaser and as a result we have no need to collect, mine, or advertise to them. We do not show any advertisements within the educational version to students.

In order to provide recommended resources we may look at data a teacher has generated to recommend activities/content to the teacher. An example would be if we detect a teacher is teaching Romeo and Juliet, we might recommend other activities for Shakespeare. This is only internal to Storyboard That, and not based on any student data, and designed specifically for the teachers.

There are some small advertisements on the site to order school-related supplies off of Amazon, Teachers Pay Teachers, or similar websites, but these are targeted towards Adults.

We can be Contacted at

Email at Contact-Us@StoryboardThat.com
Phone at +1-617-607-4259
Mailing Address:

Storyboard That
PO Box 920504
Needham, MA 02492

Personally Identifiable Information (PII)

We want to know as little as possible about our student users as we can to protect their privacy. We do not ask for email addresses when signing up in the educational version, nor is there a place to add it later. In general, it is our policy not to collect, maintain, use, or share PII beyond that needed for educational purposes, or as authorized by a parent, guardian, or student 13 years of age or older. We do not sell PII. We also do not use PII for the purpose of behavioral targeting of advertisements to students, nor for the building of personal profiles of students except as authorized by a parent, guardian, or student 13 years of age or older.

Subject to the foregoing, we collect limited personal information and other personal identifiers, as explained in in the “What Information Do We Collect” section of our Privacy Policy. As further explained in our Privacy Policy, such categories of personal information include IP addresses of users, metadata collected through the use of cookies, usernames and passwords of student users, names of student users, and content generated by students through their use of the service.

As also explained in the Privacy Policy we receive and utilize hashed information regarding email addresses.

How is Personally Identifiable Information (PII) Used

Use of PII is subject to our Privacy Policy and to the provisions explained below.

User Names

User names and display names (friendly human readable name) are shown internally within your educational account and appear in URLs for user created content. If a student has PII in their user name, either an account admin or a member of the Storyboard That staff can delete their account, or change the user name.

Storyboards, User Generated Content and Privacy

Due to the nature of Storyboard That, students every day create absolutely amazing original and creative content. By default all storyboards created under an educational account are **private**.

- The image files are stored encrypted and need a token to access them that expires after a short time period
- The URL to a storyboard will only be visible to a school teacher/admin and the student

At the sole discretion of the account administrator this security can be removed allowing the storyboard to be shared which will expose the user name and display name of a user to the internet. There is a reminder that this should only be done after verifying with your own policies and the security requirements of your students / school.

Other notes:

- It is a violation of our policies to include photos of anyone under the age of 13 (and there is a warning when uploading)
- It is a violation of our policies to provide personal information like name or address (and there is a warning when saving)

Rostering / Class Information

If the information is available, Storyboard That uses the relationship between teachers, students and classes to organize student and teacher dashboards. This allows the website to give only a subset of students in an account access to an assignment.

Data Policies

Disclosure, review, transfer, and ownership of PII is subject to our Privacy Policy and to the provisions explained below.

Downloading Storyboards

One of the best part of Storyboard That is making storyboards, and students and teachers alike have a desire to download their creations. When viewing a storyboard, a storyboard can be printed out or downloaded in a variety of digital formats. Please see our Storyboard Copyright and FAQ page for an understanding of the extensive uses we permit. *Once downloaded we have no ability to control or monitor what is in the storyboard, or how it is shared.*

Disclosing Data

Since we collect minimal PII, we have no way to contact users outside of the admin. We will happily work with a school admin to provide any and all data that is relative to their account. We will also provide any data to any valid legal, regulatory, or judicial request.

Per our Terms of Use and Privacy Policy we do use 3rd party tools like Google Analytics to aggregate site usage and performance. We are not in the business, nor do we want to be of selling student data in any way.

We will respond to the best of our abilities to basic customer service inquiries initiated by a student/parent, but we strongly prefer to work directly with the school. Basic inquiries are typically limited to “how do I do X in the storyboard creator?” Requests for more detailed information must come through the school directly.

Reviewing Personal Data

Students can review all of their work and PII from their student dashboard while logged in. If a parent / legal guardian would like to discuss anything about an account we will need the account admin to make an introduction to verify the authenticity of the request. After we know the authenticity we are happy to work to address any issues.

Transferring Data

If a student wishes to transfer their data to a personal account the process is as follows:

1. A parent/guardian must purchase a premium account
2. The school admin must notify Contact-Us@StoryboardThat.com of the user name of both the student and the new user name purchased AND
3. The school admin must tell Storyboard That to either: move data from one account to another, or to copy the data so it still also exists in the school account

    Once the accounts are linked the parent/guardian may request additional transfers of data

A student may also download their data – see (download section)

Data Ownership

We know some schools require the ownership of their data per their policies. If you require this please write in and we will mark your data as owned by you

Deleting Your Data

At any time, any school administrator can delete students and their storyboards off of our systems. We can also delete all of your data upon explicit request. After 4 years (or less at our discretion) of inactivity we will delete student data. If a parent would like their child's data deleted, that request must come through the school to verify authenticity of the request. Due to the interactive and user generated content nature of Storyboard That, user data needs to be retained for the duration of a user wanting their content.

By Default all educational accounts are set to automatically delete student data 30 days after the account has expired. This can be changed for paying users in their dashboard, or by contacting support. Every step of the deletion process sends written confirmation

Per notes elsewhere on this document the data is used for educational purposes, improving the product, and supporting customer support needs. **We do not use student data for advertising or marketing**

Backup Exception

Storyboard That is a very complicated program and uses a number of industry standard backup policies as well as maintaining error and audit logs. After deleting your data there may be historical remnants in backups that due to their snapshot nature cannot be scrubbed. The majority of these systems are automatically deleted on a regular basis, and the remainder are manually deleted on a regular basis as part of our ongoing site maintenance policies.

Data Breach

In the event of a data breach, we will notify school admins within a reasonable time period after we fully understand the impact and can effectively communicate the situation. Since we do not have contact information for students it will be up to the school/admin to notify parents.

Our Promises

- We do not create profiles of students for anything other than school purposes
- We do not sell our student data

  With an exception if we were to sell / merge the company (merger, acquisition, asset sale or similar transaction) our service and data would go to our acquirer / combined venture.
- We do not target advertisements at students
- We do not knowingly disclose student data unless that data is explicitly and intentionally made public by the school/teacher, or required by law
- At any time any administrator can delete any and all data from our systems

  Excluding backups, see above

- We do have access to view and edit your data which we use to improve our product offering (ex: by looking at which features/art are used and how), assist with customer care issues, and verify our systems are running the way we intend.
  - Any employee or contractor with access has signed an extensive NDA, and must follow our IT policies
  - Repeating our policies again, we do not sell or license this data to any third party, or use this data in any way to advertise to students

IT Security and Data Storage Practices

We use Microsoft Azure for all of our hosting and as their customer we get world class security – see for full details Azure Security. Among other protections, they provide physical security of our servers.

Answers to Common IT Security Questions

- All data transmitted between our servers, and between us and our users, is encrypted with industry-standard TLS1.2 or better.
- Data stored on our databases are encrypted at rest, secured by firewalls, and utilize encrypted channels for all connections.
- User content with privacy settings enabled is stored on encrypted drives and accessed with short-lifetime access keys.
- All internal secure systems require a username / password or greater security (including Two Factor Authentication (TFA) and/or IP Whitelists) and administrative rights.
- All employees and contractors with access to systems have undergone criminal background checks and have yearly privacy training.
- We conduct a yearly internal IT Audit using the NIST framework .

State Specific

California Schools Subject to SB-1177 (SOPIPA) and AB-1584

If you are subject to SOPIPA you may write into Contact-Us@StoryboardThat.com to:

- Have your data marked as owned by you (see data ownership)
- Have all of your data deleted on a specified date (see deletion policies)

  Note: *If you ask us to delete your data the day your account is no longer actively paying, we will have no choice but to delete all your student data. You may ask us for a "30-day hold" on data deletion to give you time to make sure there is no lapse in payment*

Connecticut State

Addendum for Connecticut only

Illinois

We are Illinois Student Online Personal Protection Act Compliant.

New York State

New York - We are Ed 2D Compliant

Washington State

Washington State - We are SUPER Act (Senate Bill 5419) Compliant

Need Help? We're Here For You!

Hello@StoryboardThat.com
+1-617-607-4259

STUDENT
PRIVACY
PLEDGE
2020 SIGNATORY