Scottsdale Unified School District #48

DATA SECURITY AND CONFIDENTIALITY AGREEMENT

This DATA SECURITY AND CONFIDENTIALITY AGREEMENT ("Data Agreement") dated 3/30/2022, by and between Scottsdale Unified School District #48 (the "District') and Clever Prototpes, LLC (DBA Storyboard That), and its subcontractors and agents (the "Service Provider").

RECITALS

A. In providing services to the District, Service Provider may have access to confidential records, data and information concerning students and employees of the District.

B. Service Provider agrees to the provisions of this Data Agreement and to the requirements of state and federal law with respect to the receipt, review, storage and transmission of information received from the District.

C. This Data Agreement shall be in addition to any underlying agreement for goods and services entered into between the parties.

NOW THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Covered Data and Information. All records, information, and data of the District to which Service Provider has access are hereafter referred to as "CDI". CDI includes, but is not limited to, all paper and electronic student education records, information and data supplied by the District, as well as any such records, information and data provided by students of the District, all personally identifiable records, information and data concerning students and employees of the District, and all personally identifiable information and other non-public information supplied, including but not limited to student data, employee data, and user content.

2. Limited Use of De-identified, aggregate or anonymized CDI. CDI does not include deidentified, aggregate or anonymized CDI. The District permits the Service Provider to use de-identified, aggregate or anonymized CDI for the purpose of research and development to improve the service offered by the Service Provider.

3. Compliance with all Applicable Laws. Service Provider agrees to comply with the requirements of The Family Educational Rights and Privacy Act (FERPA), the Pupil Protection Rights Act (PPRA), and any other federal and/or state law governing the privacy of CDI. If Service Provider processes data outside of the United States, Service Provider specifically

agrees to be bound by A.R.S. § 18-551. and -552, as amended, A.R.S. § 15-241, FERPA, PPRA and any other applicable Arizona or federal law governing CDI.

4. Access to CDI. Service Provider hereby acknowledges that the Service Provider has access to CDI and that such shall be subject to the terms and conditions of this Data Agreement. Service Provider will only collect CDI as necessary to fulfill its duties as agreed to in any underlying agreement for goods or services.

5. Use of CDI. Service Provider will use CDI only for the purpose of fulfilling its duties and providing services as agreed to in any underlying agreement for goods or services.

6. Data Mining. Service Provider is prohibited from mining CDI for any purposes other than as agreed to in writing between the parties. Data mining or scanning of user content for the purpose of advertising or marketing to anyone is prohibited. Service Provider will not use any CDI to advertise or market to anyone without express written permission of the District.

7. Confidentiality of CDI. Service Provider agrees to hold CDI in strict confidence. Service Provider shall not use or disclose CDI received from or on behalf of the District except as permitted or required by this Data Agreement, as required by law, or as otherwise authorized in writing by the District. Service Provider agrees that it will protect CDI it receives from or on behalf of the District according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

8. Data De-Identification. Service Provider may have permission via any underlying agreement to provide goods or services to use de-identified CDI for purposes as identified in the agreement. De-identified CDI will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, identification numbers, date of birth, demographic information, location information and school identification numbers. Service Provider agrees not to attempt to re-identify de-identified CDI and agrees not to transfer de-identified CDI to any party without permission. Any receiving party shall agree in writing not to attempt re-identification and shall agree to be bound by the terms of this Data Agreement.

9. Reporting Student CDI. Service Provider may at times have reason to report CDI of District students to third parties as provided by express written permission from the District or as required by law. In reporting aggregated, de-identified data containing CDI, Service Provider shall:

    a. Not disclose data about categories of 10 or fewer students;

    b. Not report a total count of students;

    c. Not report percentages of 0% or 100%; and

    d. Report data in ranges rather than specific numbers.

10. Return or Destruction of CDI. Upon termination, cancellation, expiration or other conclusion of the work or services provided to the District by Service Provider, Service Provider shall return all CDI to the District. If the return of CDI is not feasible, Service Provider shall destroy any and all CDI and represent in writing to the District that it has destroyed all CDI and no longer has any CDI in its possession or control. Service Provider shall ensure that all CDI it is possession or the possession of any subcontractors or agents is destroyed or returned to the District when no longer needed for the specified purposes as authorized by the District.

11. Security of Electronic Information. Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures and technical safeguards to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from or on behalf of the District or its students or employees. Service Provider shall store and process CDI in accordance with industry best practices to secure CDI from unauthorized access, disclosure and use. These security measures and technical safeguards shall be extended by express written agreement to all subcontractors and third parties used by Service Provider. Service Provider shall at a minimum:

    a. Protect and maintain the confidentiality of passwords used to access CDI;

    b. Notify the District when Service Provider's access to CDI is no longer necessary;

    c. Notify the District within two days of discovery if passwords used to access CDI by Service Provider, a subcontractor, or other third party are lost, stolen, or otherwise obtained or potentially obtained by unauthorized users.

    Service Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

12. Reporting of Disclosure or Misuse of CDI. Service Provider shall, within 72 hours, report to the District any and all use or disclosure of CDI not authorized by this Data Agreement or authorized in writing by the District. Service Provider's report shall identify:

    a. The nature of the unauthorized use or disclosure;

    b. The CDI used or disclosed;

    c. The identity of the person or entity who made the unauthorized use or received the unauthorized disclosure;

    d. What Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and

    e. What corrective action Service Provider has taken or shall take to prevent further similar unauthorized use or disclosure.

Service Provider shall provide such other information, including a written report, as reasonably requested by the District. Service Provider shall have a plan for responding to a breach of data security developed pursuant to best practices in the industry and shall share that plan with the District upon request.

13. District Access. Any CDI held by Service Provider will be made available to the District upon request.

14. Rights to Intellectual Property. This Data Agreement does not give Service Provider any rights, implied or otherwise, to CDI, data, content or intellectual property except as expressly stated in any underlying agreement between the parties. This includes but is not limited to the right to share, sell or trade CDI. The District acknowledges that this agreement does not convey any intellectual property right in any of Service Provider's materials or content, including any revisions of derivative work or material. Service Provider-owned materials shall remain the property of the Service Provider. All rights, including copyright, trade secrets, patent and intellectual property rights shall remain the sole property of the Service Provider.

15. Indemnity. Service Provider shall defend and hold the District, its Board Members, officers, agents and employees, harmless from all claims, liabilities, damages or judgments involving a third party, including the District's costs and reasonable attorneys' fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Data Agreement. Service Provider shall also comply with the breach notification requirements under applicable law that arise from the result of Service Provider's failure to meet any of its obligations under this Data Agreement.

16. Remedies. If the District determines in good faith that Service Provider has materially breached any of its obligations under this Data Agreement, the District shall have the right to require Service Provider to submit to a plan of monitoring and reporting; to provide Service Provider with a fifteen (15) day period to cure the breach; or to terminate the work or services of Service Provider for the District immediately. Prior to exercising any of these options, the District shall provide written notice to Service Provider describing the violation and the action the District intends to take. The remedies described herein may be exercised by the District in its sole discretion and are in addition to any remedies permitted by law or pursuant to any other agreement between the parties.

17. Subcontractors. Service Provider shall require that any subcontractor or agent receiving CDI is authorized by the District to receive CDI and that the subcontractor or agent expressly agrees to be bound to the terms of this Data Agreement.

18. Modifications. Service Provider will not modify or change how CDI is collected, used or shared under the terms of this Data Agreement in any way without advance notice to and consent from the District.

19. Arizona Law. This Data Agreement is made in the State of Arizona and shall be interpreted by the laws of the State of Arizona. Any dispute arising out of or relating to this Data Agreement shall be brought in the Maricopa County Superior Court or the United States District Court, District of Arizona.

20. Cancellation. The District reserves all rights that it may have to cancel this Data Agreement for possible conflicts of interest under A.R.S. § 38-511, as amended.

21. Arbitration. To the extent permitted by A.R.S. §§12-1518 and 12-133, the parties agree to resolve any dispute arising out of this Agreement by arbitration.

22. Amendments. All references to provisions of statutes, codes and regulations include any and all amendments thereto.

23. Miscellaneous. The provisions of this Data Agreement shall survive the termination, cancellation or completion of all work, services, performance or obligations by Service Provider to the District. This Data Agreement shall be binding upon the parties hereto, their officers, employees and agents. Time is of the essence of this Data Agreement. Except as expressly modified by the provisions of this Data Agreement, any underlying agreement for goods or services shall continue in full force and effect. In the event any inconsistencies exist between the terms of this Data Agreement and any underlying agreement, this Data Agreement shall control.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed by its authorized parties on its behalf.

Scottsdale Unified School District #48

DocuSigned by:
By: Dr. Kimberly Guerin
6A59EE39359E4EE...

Printed Name: Dr. Kimberly Guerin

Title: Assistant Superintendent

Date: 3/30/2022

Clever Prototypes, LLC (DBA Storyboard That):

DocuSigned by:
By: Aaron Sherman
40952C4C3532484...

Printed Name: Aaron Sherman

Title: CEO

Date: 3/30/2022

Student Privacy and Storyboard That

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