

Data Privacy and Security Plan (NY § 2-d)

The text in bold is quoted directly from NY Education Law §2-d. The following text is an explanation of how Tools For Schools Inc meets or exceeds these requirements.

1. **Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;**

Our mission to empower the next generation of creators includes some important principles about how we safeguard the data you entrust to us.

We are COPPA, FERPA and GDPR compliant: Book Creator is fully compliant with these important laws and we're proud to have achieved COPPA and FERPA certification from the Internet Keep Safe Alliance.

Teachers are always in control: For example, a student's book is private by default. Only teachers can choose to share a book with a wider audience.

We don't sell user data or advertise: We will never advertise or sell data about you. Our business model is simple – we charge for access to Book Creator.

We protect your information: We use security industry best practices, such as encryption of your data in transit and at rest. All data is stored in Google Cloud offering the best security in the world.

Ownership of content: Your books belong to you, and you can download them at any time.

2. **specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;**

All employees are vetted for working with student data.

Continuous security compliance audit conducted by Drata. This includes user access review, information security policy adherence and both static and

dynamic application security scans. We are aiming for SOC2 Type II certification by end of 2024.

Regular penetration tests conducted (at least annually).

Data is encrypted at-rest and in-transit using industry standard mechanisms - see <https://cloud.google.com/security/>

Access to systems that store, process or transmit data is controlled by a role-based access system. Users are authenticated by this system using a strong password and two-factor authentication (not SMS-based).

Regular employee training (internally and by iKeepSafe) to ensure awareness of, and compliance with, COPPA, FERPA, GDPR, NY Education Law 2-d.

All data is stored in Google-owned datacenters in the continental US. Detailed information about the administrative, technical and organisational protections can be found here: <https://cloud.google.com/security/>.

The Book Creator terms and privacy policy can be found here: <https://bookcreator.com/privacy-policy/>

All data in flight sent using SSL/TLS. See <https://cloud.google.com/security/encryption-in-transit/> for more details.

Encryption at rest is AES 128/256 provided by Google Cloud: <https://cloud.google.com/security/encryption-at-rest/>.

3. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

Some information is included below to help the educational agency develop the supplemental information for the parents bill of rights for data privacy and security for Tools for Schools Inc.

1. the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

We use student/teacher/principal data to:

- provide Book Creator and make sure you can use it properly and effectively;
- manage and administer your account and the books that you create;

- respond to any questions, requests or complaints we receive from you;
- communicate with you about Book Creator if we need to;
- investigate potential illegal activities on Book Creator;
- analyse use of Book Creator; and
- to improve Book Creator.

We will never use your information to target advertising at you based on your behavior. We will not build a personal profile of you other than for supporting authorised educational or school purposes, or as authorised by you (or by a parent or guardian if necessary). We also won't use your information for any purposes except those above without letting you know and getting your permission if necessary.

More information here: <https://bookcreator.com/pp-us/>.

- 2. how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);**

Any and all sub-contractors are engaged in such way as to preserve the same obligations and protections outlined in this plan.

- 3. the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).**

Upon termination or expiry of the contract, data can be destroyed on written request; or returned to the educational agency within 30 days of written request as JSON data and ePub 3.0 book files.

4. if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; including technical support;

A teacher or principal may challenge the accuracy of the data by contacting our support team by visiting <https://support.bookcreator.com/> and selecting "Chat with the Book Creator team", or using the in-app chat button.

Suewan Kemp, Support Operative

Mail: 1321 Upland Dr., Suite 8524, Houston, TX 77043.

Phone: 877-366-5116

A parent, student or eligible student may challenge the accuracy of the data by contacting the educational agency who will contact Tools for Schools on their behalf.

5. where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and

All data is stored in Google Cloud data-centers in the continental US. Detailed information about the administrative, technical and organisational protections can be found here: <https://cloud.google.com/security/>.

The Book Creator terms and privacy policy can be found here: <https://bookcreator.com/privacy-policy/>

6. address how the data will be protected using encryption while in motion and at rest.

All data in flight sent using SSL/TLS. See <https://cloud.google.com/security/encryption-in-transit/> for more details.

Encryption at rest is AES 128/256 provided provided by Google Cloud: <https://cloud.google.com/security/encryption-at-rest/>.

4. specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data

receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

All employees who have access to student data are required to take annual training on their obligations under FERPA and COPPA as provided by iKeepSafe.

All employees who have access to student data are required to take annual training on their obligations under NY Education Law §2-d.

All employees who have access to student data are required to take annual training NIST Cybersecurity and Privacy Framework v1.1.

5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

Any and all sub-contractors are engaged in such way as to preserve the same obligations and protections outlined in this plan.

6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

We maintain an operational Incident Reporting Policy - copy available on request.

7. describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Upon termination or expiry of the contract, data can be returned to the educational agency, within 30 days of a written request, as JSON data and ePub 3 book files.

We may transfer data to a successor contractor. We may transfer our rights and obligations under these terms to another organisation. We will contact you to let you know if we plan to do this. If you are unhappy with the transfer you may contact us to end the contract within 30 days of us telling you about it.

More details are in Section 11 of our standard terms and conditions:
<https://bookcreator.com/terms-of-service/>

Data is removed from servers using NIST compliant secure deletion.
Certification of deletion available on written request.

Supplemental information

Data Protection Officer: Thom Leggett, thom@bookcreator.com

Main point of contact for service contract: David Swift, david@bookcreator.com

NIST Cyber Security Framework 1.1

Our internal practices align with NIST CSF v1.1 Framework
(<https://www.nist.gov/cyberframework/new-framework>).

Reference

The full legal text of NY 2-d for reference:

[part-121.pdf](#)