

AGREEMENT REGARDING DATA SECURITY AND PRIVACY

This Agreement regarding Data Security and Privacy (“Agreement”) dated as of 5/23, 2025, by and between the Greater Southern Tier BOCES (“District”) and CK-12 Foundation (“Contractor”). This Agreement covers only student accounts sanctioned by the district and set up through the @gstboces.org domain(s).

WHEREAS, the District has licensed certain services or products from Contractor, pursuant to and as identified in Contractor’s Terms of Use, found at www.ck12info.org/about/terms-of-use/ (“Contractor TOU”), which is incorporated herein as may be amended; and

WHEREAS, Contractor is a third-party contractor as defined in Part 121 of the Commissioner’s Regulations, that will receive student data or teacher or principal data from the District pursuant to “Contractor TOU,” and this Agreement for purposes of providing services to the District; and

WHEREAS, the parties agree that if any provision of this Agreement conflicts with a provision of “Contractor TOU,” the provision as set forth in this Agreement shall supersede and prevail over said other provision;

NOW, THEREFORE, in consideration of the mutual covenants, conditions and agreements contained herein, and for other good and valuable consideration, including the above-referenced “Contractor TOU,” the Contractor and the District hereby agree as follows:

A. The Contractor shall comply with all state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the Parents’ Bill of Rights, hereinafter referred to as “Attachment A,” and Supplemental Information, annexed hereto and herein after referred to as “Attachment B.”

B. The Contractor may receive personally identifiable information from student records (“Education Records”) and/or personally identifiable information from annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release pursuant to Education Law § 3012-c and 3012-d (collectively, “PII Data”). The Contractor shall, therefore, comply with the following provisions in order to maintain the security and confidentiality of personally identifiable information:

- (i) adopt technologies, safeguards and practices in alignment with the NIST Cybersecurity Framework;
- (ii) limit the Contractor’s internal access to Education Records to individuals with legitimate educational interests;
- (iii) use PII Data only for the purposes explicitly authorized by this Agreement and not for any other purpose;
- (iv) not disclose any personally identifiable information from PII Data to any other party without prior written consent, unless disclosure is required by statute or court order and written notice is given to the District (notice is not required if it is expressly prohibited by a statute or court order);

- (v) maintain reasonable safeguards to maintain confidentiality of personally identifiable information in PII Data;
- (vi) use legally mandated encryption technology¹ to protect data from unauthorized disclosure while the data is in motion or in the contractor's custody; and
- (vii) not sell, use or disclose student, teacher or principal personally identifiable information for any marketing or commercial purpose.
- (viii) For the avoidance of doubt, it is expressly understood and agreed that Education Records do not include students' "User Content," as defined in the "Contractor TOU."

C. The Contractor represents and warrants that it will follow and abide by the guidelines and legal standards as set forth in the Contractor's data security and privacy plan as attached hereto as "Attachment C."

The Contractor's data security and privacy plan shall, at a minimum:

- (i) outline how the Contractor will implement State and federal data security and privacy contract requirements for the life of the contract;
- (ii) specify administrative, operational and technical safeguards the third-party contractor will use to protect personally identifiable information;
- (iii) show that it complies with requirements of §121.3(c) of the Commissioner's Regulations;
- (iv) specify how the third-party contractor's employees and any assignees with access to student data, or teacher or principal data receive or will receive training on relevant confidentiality laws, before receiving access to such data;
- (v) specify if the third-party contractor will use subcontractors and how it will ensure personally identifiable information is protected;
- (vi) specify an action plan for handling any breach or unauthorized disclosure of personally identifiable information and promptly notify the school district of any breach or unauthorized disclosure; and
- (vii) describe whether, how and when data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated.

D. The Contractor must notify the District of any breach of security resulting in an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employee's, assignees or subcontractors. This notification must be made in the most expedient way possible and without delay. In addition, the Contractor must notify the District of the breach of security in writing. This written notification must be sent by the Contractor in the most expedient way possible and without unreasonable delay, and not later than seven (7) calendar days after confirmation of the breach of security resulting in an unauthorized release of personally identifiable information from PII Data, to the designated District representative and will be delivered to the District by electronic mail to Edward White, Data Protection Officer, DPO@gstboces.org. In the case of an unauthorized release of personally identifiable information from PII Data by the

¹ Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

Contractor or the Contractor's officers, employees, assignees or subcontractors, the Contractor will reimburse the District for the reasonable cost to fulfill the District's obligation to notify any required party pursuant to NYCRR 121.10(f), subject to any limitation of liability agreed to in Contractor's TOU. For the avoidance of doubt, this reimbursement obligation does not include any other costs or losses related to responding to a breach of security (e.g. District legal fees, notification under other statutes).

E. The Contractor and District agree that this Agreement and the Attachments included hereto supersede and replace any previous agreements or contracts between the parties.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

DISTRICT: Greater Southern Tier BOCES	CONTRACTOR: CK-12 Foundation
BY: <i>Edward R White III</i> Edward White III, Data Protection Officer	BY: Miral Shah, Chief Technology & Product Officer DocuSigned by:  81C4BF5FA844CF...
DATE: 5/23/202	DATE: 5/29/2025

ATTACHMENT A
PARENTS' BILL OF RIGHTS FOR
STUDENT DATA PRIVACY AND SECURITY

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

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

federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

ATTACHMENT B
PARENTS' BILL OF RIGHTS FOR
STUDENT DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

In accordance with its obligations under the Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

(1) The student data or teacher or principal data (collectively, "PII Data") received by the Contractor will be used exclusively for the following purpose(s):

Contractor and its agents, employees and subcontractors, if any, shall use PII Data solely for the purpose of providing services as set forth in the "Contractor TOU," and this Agreement. Contractor and its agents, employees and subcontractors will not use PII Data for any other purposes. Any Data received by Contractor or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

(2) The Contractor will ensure the confidentiality of PII Data that is shared with subcontractors or other persons or entities as follows:

In the event that Contractor subcontracts with an outside entity or individual in order to fulfill its obligations to the District, Contractor ensures that it will only share PII Data with such subcontractors as described as "Third Party Service Providers" in "Attachment C" section (v) who maintain such data privacy and security consistent with those required of Contractor pursuant to the Agreement. Contractor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII Data in its custody consistent with the data protection and security requirements of state and federal law and regulations by adhering to the provisions in the "THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN," "Attachment C."

(3) This Agreement is effective upon execution by both parties and shall continue until terminated by either party by giving at least 30 days written notice. Within thirty (30) calendar days after the termination of the Agreement, all PII Data will be de-identified and/or deleted from Contractor's computer systems, based on written request from the District. Contractor will provide written confirmation of such disposition to the District, upon written request.

(4) A parent, student, teacher or principal can challenge the accuracy of PII Data received by the Contractor as follows:

In the event that a parent or eligible student wishes to challenge the accuracy of PII Data concerning that student that is maintained by Contractor or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Contractor is notified of the outcome of any such

errors made by Contractor, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The District or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Contractor or its subcontractors.

(5) The following is how PII Data will be stored and what security protections will be taken by the Contractor:

All Data in Contractor's possession will be securely stored. Contractor represents that the following security protections, including encryption where applicable, will be in place to ensure that PII Data is protected.

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls

ATTACHMENT C
THIRD-PARTY CONTRACTOR'S
DATA SECURITY AND PRIVACY PLAN

In accordance with its obligations under the Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

- (i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract by:

Adhering to the NIST Cybersecurity Framework. Our NIST "Current Profile" is available upon request.

- (ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:

Refer to Section 11 of the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>

- (iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information as follows:

§121.3(c)(1)

- Refer to Section 5 in the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>

§121.3(c)(2)

- Refer to Section 6 in the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>

§121.3(c)(3)

- For contract duration, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above.

- For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above, and to Sections 8 and 13 in the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>

§121.3(c)(4)

- Refer to item 4 in the Parents' Bill of Rights above.

§121.3(c)(5)

- The CK-12 site runs on the Amazon Web Services (AWS) cloud.

- Refer to Section 13 in the CK-12 Privacy Policy, found at

<https://www.ck12info.org/privacy-policy/>, for more information on security.

§121.3(c)(6)

- Refer to Section 13 in the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>

- (iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

Employees with access to PII receive training on handling this data.

- (v) Contractor works with third party service providers for cloud-based hosting, communicating with users for product support and information, troubleshooting issues, and analytics.

For more information on any of the third parties used by Contractor, please email: support@ck12.org

- (vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:

CK-12 has an established incident response plan, which can be provided upon request.

- (vii) Data will be returned, transitioned to a successor contractor, deleted, de-identified, or destroyed when the contract ends or is terminated as follows:

- For disposition or transfer of data, refer to item 3 in the Supplement to the Parents' Bill of Rights, "Attachment B," above, and to Section 6 in the CK-12 Privacy Policy, found at <https://www.ck12info.org/privacy-policy/>