

Gilboa-Conesville Central School

132 Wyckoff Road • Gilboa, New York 12076-9703

607-588-7541 • FAX 607-588-6820

Bonnie Johnson, Superintendent

Jacqueline Frederick, K-6 Principal Mary Hinkley, 7-12 Principal

Gilboa-Conesville Central School District Parents' Bill of Rights for Data Privacy and Security

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c and §3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or principal data will be sold or released for any commercial purpose;
2. Parents have the right to inspect and review the complete contents of their child's education records.
Procedures for reviewing student records can be found in the Board Policy §736Q
3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;
4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/inventory-of-data-elements-collected-by-nysed_0.pdf or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New

York 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed.

Complaints should be directed to Denise Rose, Data Protection Officer;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

- Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
- Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
- The District will require complaints to be submitted in writing;
- The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data. The supplemental information must be developed by the District and include the following information:

- 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;
- 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);
- 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 District, and whether, when and how the data will be destroyed);
- 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;
- where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third-party contractor where the third-party contractor receives student data or teacher or principal data.

Appendix

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Gilboa Conesville Central School has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data" as those terms are defined by law.

Each contract GCCS enters into with a third-party contractor, where the third-party contractor receives student data or teacher or principal data, will include the following information:

- The exclusive purposes for which the student data or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
- When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.

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.

- Where the student, 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, including whether such data will be encrypted.

This section to be completed by the Third-Party Contractor and returned to Gilboa-Conesville CSD

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

☒ **Yes**

Please complete Sections 2, 3 and 4

☐ **No**

Please complete Section 3

Section 2: Supplemental Information Details

Third-Party Contractors subject to New York Education Law § 2-d- please complete the table below:

SUPPLEMENTAL INFORMATION ELEMENT SUPPLEMENTAL INFORMATION

Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract [or list the section(s) in the contract	Topical Review Book Company provides an interactive eBook platform. We produce books that cover the curriculums in Math, Science, English,
---	--

<p>where this information can be found]</p>	<p>and Social Sciences. The cloud-based accounts are set up by a school administrator, with assistance from our in-house experts, using emails and passwords which the school provides. Our reader is compatible with Google Classroom and integrates with most major LMS platforms through LTI and API options, including Blackboard, Canvas, Moodle, and many others. Individuals can access their accounts on up to 3 different platforms, i.e. tablets, phones, and computers anywhere they have internet service.</p>
<p>Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract [or list the section(s) in the contract where this information can be found]</p>	<p>If subcontractors are engaged, the following measures will be in place:</p> <ul style="list-style-type: none"> • The subcontractor will be required to sign a Data Privacy and Security Addendum, agreeing to the same privacy and security terms outlined in this plan. • Topical Review Book Company will monitor and audit subcontractors to ensure compliance with data protection requirements. • The subcontractor will be trained on the confidentiality of Protected Information. <p>Topical Review Book Company currently uses Kitaboo and AWS for our interactive eBook Reader App. Kitaboo is a subsidiary of Hurix Corp, based in Plano Texas. AWS is owned by Amazon. Topical Review Book Company and Kitaboo do not store any student personal information beyond the login credentials (email and passwords). Topical Review Book Company does have an agreement with Kitaboo that contains data privacy and security requirements at least as stringent as those required by the DOE in this agreement. Our agreement with AWS is for the cloud storage of our eBooks only.</p>
<p>Please list when the agreement expires and what happens to the protected data when the agreement expires [or list the section(s) in the contract where this information can be found]</p>	<p>Upon termination or expiration of the contract, unless an extension or renewal is in process, Topical Review Book Company will:</p> <ul style="list-style-type: none"> • Return all Protected Information or transition it to a successor contractor. • Securely delete or destroy any remaining Protected Information, ensuring that no residual

	<p>data is recoverable.</p> <ul style="list-style-type: none"> • Certify in writing that all Protected Information has been returned, deleted, or destroyed in accordance with this plan. • Topical Review Book Company will not collect or use any deidentification data for any purpose. Data destruction will be performed in a manner consistent with industry best practices to ensure that all Protected Information is irrecoverable. Including the deletion of hard drives and backups, shredding of physical material, and any other deletion necessary.
<p>Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how [or list the section(s) in the contract where this information can be found]</p>	<p>Submit complaints to the NY State Education Department (NYSED):</p> <ul style="list-style-type: none"> -Online:http://www.nysed.gov/data-privacysecurity/report-improper-disclosure - By email: CPO@mail.nysed.gov - By mail: Chief Privacy Officer New York State Education Department 89 Washington Avenue, Albany NY 12234 - By phone at: 518-474- 0937 <p>Submit complaints to Topical Review Book Company</p> <ul style="list-style-type: none"> - By email: info@Topicalrbc.com - By mail: Chief Privacy Officer Topical ReviewBook Company P.O. Box 328 Onsted MI 49265
<p>Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated [or list the section(s) in the contract where this information can be found]</p> <p>Please list how the data will be protected using encryption [or list the section(s) in the contract where this information can be found]</p>	<p>Administrative Safeguards:</p> <ul style="list-style-type: none"> o Access controls: Only authorized personnel will have access to Protected Information. o Data handling procedures: All employees will adhere to strict guidelines regarding the handling, sharing, and storage of Protected Information. o Incident response plan: A clear process for responding to data security incidents, including breaches and unauthorized disclosures. <p>Operational Safeguards:</p> <ul style="list-style-type: none"> o Role-based access: Access to Protected Information will be granted based on job responsibilities. o Regular data audits: Periodic audits will be

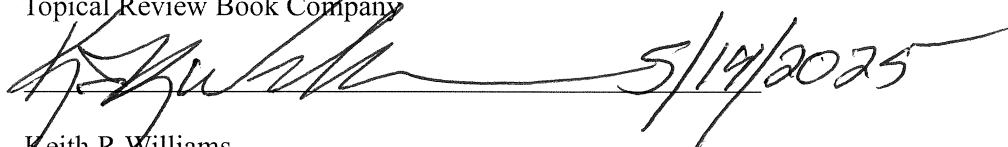
	<p>conducted to ensure compliance with the data security and privacy policies.</p> <ul style="list-style-type: none"> o Secure data transfer: Encrypted channels will be used for the transfer of Protected Information. <p>Technical Safeguards:</p> <ul style="list-style-type: none"> o Encryption: All Protected Information will be encrypted both in transit and at rest. o Secure storage: Protected Information will be stored in secure systems that meet industry standards. o Firewalls and intrusion detection systems: These will be deployed to protect against unauthorized access and cyberattacks.
--	---

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Gilboa-Conesville CSD Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Topical Review Book Company



Keith R Williams

President

Section 4: Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-0

Gilboa-Conesville Central School and the Third-Party Contractor agree as follows:

1. Definitions:

- Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
- Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and Gilboa-Conesville Central School's Data Security and Privacy Policy:

3. The Parties agree that Gilboa-Conesville Central School's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;
4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations
5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;
6. The Third-Party Contractor shall:
 - a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
 - b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
 - c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
 - i. without the prior written consent of the parent or eligible student; or
 - ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
 - d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
 - e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified 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;
 - f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework; g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

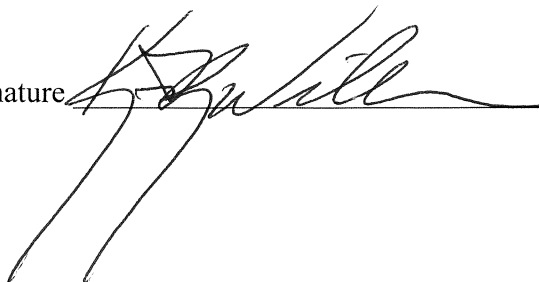
Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Topical Review Book Company

Printed Name Keith R Williams

Signature



Date

5/14/25