

Data Privacy Agreement

This Agreement is entered into between the **Roseville City School District** ("LEA" or "District") and

Jigsaw Learning LLC, dba TeachTown

"Service Provider" or "Vendor"

("Service Provider" or
"Vendor") on

10/20/2026

Effective Date

WHEREAS, the LEA and the Service Provider entered into an agreement for educational or digital services to the LEA;

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; and

WHEREAS, the provider and LEA agree that additional and modified sections are required to address the use of Artificial Intelligence ("AI") as part of the services or product provided;

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.

Vendor Attestation:

Agree

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.

Vendor Attestation:

Agree

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 protected and confidential. Release of this data can be authorized only by Technology Services management and by state and federal law.

Vendor Attestation:

Agree

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.

Vendor Attestation:

Agree

5. TRANSPORT: The 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.

Vendor Attestation:

Agree

6. EXTERNAL SECURITY: The 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.

Vendor Attestation:

Agree

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 personnel (or their representatives) will have directly with District data. How is the data uploaded 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 protect against unauthorized access to District data? How are backups performed, and who has access to and custody of the backup media? How long are backups maintained? What happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard-copy records?

Vendor Attestation:

Agree

8. DISTRICT ACCESS: The 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).

Vendor Attestation:

Agree

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. The Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Vendor Attestation:

Agree

Section II: AB1584 Compliance - Student Information Only

1. The Vendor agrees that the Roseville City School District retains ownership and control of all student data.

Vendor Attestation:

Agree

2. The Vendor must attach a description of how student-created content can be exported and/or transferred to a personal account to this document.

Vendor Attestation:

Agree

3. The Vendor is prohibited from allowing third parties access to student information beyond those purposes defined in the contract.

Vendor Attestation:

Agree

4. The Vendor must attach a description of how parents, legal guardians, and students can review and correct their personally identifiable information to this document.

Vendor Attestation:

Agree

5. The Vendor will attach to this document evidence of how student data is kept secure and confidential.

Vendor Attestation:

Agree

6. The Vendor will attach to this document a description of the procedures for notifying affected parents, legal guardians, or eligible students when student records are unauthorizedly disclosed.

Vendor Attestation:

Agree

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled.

Vendor Attestation:

Agree

8. The Vendor will attach to this document a description of how they and any third-party affiliates comply with FERPA.

Vendor Attestation:

Agree

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students.

Vendor Attestation:

Agree

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.

Vendor Attestation:

Agree

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Vendor Attestation:

Agree

3. Vendors cannot sell student information.

Vendor Attestation:

Agree

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety, or operational improvement reasons.

Vendor Attestation:

Agree

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Vendor Attestation:

Agree

6. Vendors must delete district-controlled student information when requested by the District.

Vendor Attestation:

Agree

7. Vendors must disclose student information when required by law, for legitimate research purposes, and for school purposes to educational agencies.

Vendor Attestation:

Agree

Section IV: Audit and Compliance Oversight

1. Audit Rights. The District reserves the right to audit the Vendor's privacy and security practices no more than once annually or at any time in response to a data incident, suspected noncompliance, or legal/regulatory inquiry. The Vendor shall provide reasonable access to systems, records, and personnel involved in the handling of District data.

2. Confidentiality Agreement. RCSD agrees to execute a reasonable non-disclosure agreement to protect Vendor trade secrets or proprietary information disclosed during the audit.

3. Framework Compliance. Vendor agrees to implement and maintain security controls consistent with one or more of the following frameworks:

- a. NIST Cybersecurity Framework (NIST CSF)
- b. NIST SP 800-53 or 800-171
- c. ISO/IEC 27001
- d. CIS Critical Security Controls (Top 18)

The Vendor shall indicate which framework is used and provide a summary upon request.

Designated Security Framework(s):

NIST Cybersecurity Framework (NIST CSF) & AICPA SOC 2 Type 2. TeachTown formally aligns its operational processes, asset management, risk management, and incident handling protocols with the NIST Cybersecurity Framework (NIST CSF), as well as NIST SP 800-61 (Incident Handling) and NIST SP 800-88 (Media Sanitization). Furthermore, TeachTown undergoes annual independent audits and maintains an active SOC 2 Type 2 Certification covering the Trust Services Criteria for Security.

4. Security Program Documentation. Upon request, the Vendor shall furnish RCSD with the following:

- a. A summary of its data security policies and incident response procedures.
- b. Results from the most recent third-party security assessment or audit, redacted as necessary.
- c. Any certifications (e.g., SOC 2, ISO 27001).

5. Remediation Obligations. If a security deficiency or compliance failure is identified, the Vendor shall deliver a written remediation plan to RCSD within thirty (30) days. The District may suspend access to its data until the deficiency is addressed to the District's satisfaction.

6. Subprocessor Oversight. The Vendor is responsible for ensuring that all subprocessors or affiliates with access to District data comply with the terms of this agreement and are subject to equivalent audit and compliance obligations.

Exhibits

Section 1.6: External Security

TeachTown operates its cloud-hosted Software as a Service (SaaS) within Amazon Web Services (AWS) data centers located in the United States. To protect against external hacking, intrusion, and perimeter attacks, TeachTown implements a defense-in-depth security architecture:

Web Application & Network Firewalls: Systems are guarded by AWS Web Application Firewalls (WAF), network firewalls, and host-based firewalls with strict port and protocol restrictions.

Active Monitoring & Intrusion Detection: Systems are continuously monitored 24/7/365 by an independent Managed Security Service Provider (MSSP) Security Operations Center (High Wire Networks SOC) utilizing Security Information and Event Management (SIEM) logging and Endpoint Detection and Response (EDR) software.

Vulnerability Scanning: External and credentialed vulnerability scans are conducted weekly using AWS scanning technologies. An independent third party performs annual risk assessments and maintains a risk register.

Independent Attestation: TeachTown maintains an active SOC 2 Type 2 certification audited by Bonadio & Co., LLP covering the Security Trust Services Criteria.

Section 1.7: Internal Security

TeachTown enforces strict internal security controls governing data handling, processing, and administrative access:

Access Control & IAM: Access to student data requires valid credentials and is governed by Role-Based Access Control (RBAC) and AWS Identity and Access Management (IAM) under least-privilege principles. Remote administrative access requires a Virtual Private Network (VPN) connection with unique user IDs, strong passwords, and mandatory two-factor authentication (2FA). Sessions expire after 60 minutes of inactivity.

Personnel Vetting & Training: All full-time personnel undergo criminal background checks, screening, and reference checks prior to hire, as well as mandatory annual cybersecurity and privacy training.

Data Processing & Backups: Roster data pushed via Clever, ClassLink, or HTTPS is processed into encrypted database stores using TLS 1.2 / AES-256 protocols. Automated daily backups to AWS are encrypted at rest. Automated nightly database restorations are performed against the reporting environment to verify backup integrity.

Data Disposal & Media Sanitization: Virtual Desktop Interfaces (VDI) ensure non-production data never leaves the cloud environment. Storage nodes and physical media are sanitized in accordance with NIST SP 800-88 standards.

Section II.2: Exporting of Student-Created Content

TeachTown's enCORE and Launch for PreK learning platforms capture student responses, activity data, IEP goal progress, and assessment work within centralized database stores. District educators and authorized facilitators have continuous, real-time access to extract, filter, and download student progress reports, IEP tracking logs, and unit assessment summaries at any time. Reports can be exported in parent-friendly PDF formats suitable for sharing with parents, transferring to personal accounts, or filing in cumulative educational records.

Section II.4: Review and Correct Personally Identifiable Information (PII)

Parents, legal guardians, and eligible students can inspect student record information, demographic fields, and performance metrics through parent-friendly progress reports provided by classroom facilitators or during IEP conferences. If an error or inaccuracy is identified, the parent/guardian submits a request to the designated District Account Administrator or classroom teacher. Authorized district facilitators utilize the TeachTown administration portal to review, edit, correct, or amend student PII records directly.

Section II.5: Securing Student Data

TeachTown secures student data through comprehensive technical, physical, and administrative safeguards:

Encryption: TLS 1.2 (AES-256) for data in motion; NIST-compliant AES-256 for data at rest. Passwords stored using salted one-way hashes.

System Security: AWS cloud data centers, AWS WAF, EDR anti-malware, host firewalls, and central MDM device encryption.

Operational Controls: 24/7 MSSP SOC log monitoring, weekly vulnerability scanning, annual third-party risk assessments, and annual employee privacy training.

Compliance Evidence: Active SOC 2 Type 2 Report and Technical & Security Overview documentation.

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

TeachTown complies fully with FERPA by operating under the "School Official" exception with legitimate educational interests as designated by the LEA. Student PII is collected, processed, and stored strictly for authorized educational purposes on behalf of the district. TeachTown never sells, rents, or uses student data for commercial profiling or targeted advertising. Subcontractors and subservice organizations are contractually bound to maintain equivalent FERPA-compliant confidentiality and privacy protections.

Section III.5: How Student Data is Protected:

TeachTown ensures complete compliance with California SB 1177 (SOPIPA) through enforced technical and policy controls:

Technical Safeguards: Student data is completely isolated from advertising networks. Controls include TLS 1.2 / AES-256 encryption, mandatory 2FA VPN for administration, 60-minute session expiration, automated daily encrypted backups, and NIST SP 800-88 media sanitization upon deletion requests.

Administrative Controls: Annual employee privacy training, formal Incident Response Plan aligned with NIST SP 800-61, vendor due diligence, and risk register management.

Contractual Guarantees: Strict prohibitions against targeted advertising, commercial profiling, data mining, or selling student records.

Required Security & Compliance Attachments

Please upload all required documentation referenced in this agreement, including evidence of external and internal security controls, data protection practices, compliance certifications (e.g., SOC 2, ISO 27001), incident response procedures, and any required FERPA, SOPIPA, or AB 1584 compliance documentation.

Attachments should clearly correspond to the sections outlined in the Data Privacy Agreement.

Upload

[Private File Not Included]

[Private File Not Included]

[Private File Not Included]

[Private File Not Included]

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

Section A: Applicability Declaration

Please select the appropriate response below:

- ☐ Option 1: Applicable (AI Deployment Active) ☒ Option 2: Not Applicable (No AI Deployment)

Option 1: Applicable (AI Deployment Active)

The Service Provider currently uses, embeds, or leverages AI features, models, or third-party AI sub-processors to deliver Services to the District.

- **Required:** Provider must comply with all sections of this Addendum.
- **Action:** Review all requirements and execute the signature block below.

Option 2: Not Applicable (No AI Deployment)

The Service Provider does not currently use, embed, or leverage AI features or third-party AI services in connection with District Student Data or Services.

- **Waived:** Sections 1 and 3–10 do not apply.
- **Required:** Provider must comply with Section 2.1 (Future Deployment Notification).
- **Action:** Sign the signature block below to execute this waiver.

Section B: AI Governance Terms

1. AI Usage Limitations, Ownership & Third-Party Models

- 1.1.** The Service Provider shall not use, transfer, or reproduce Student Data for Artificial Intelligence (AI) training, model development, fine-tuning, or content generation without the District's prior written consent. The Provider agrees to uphold the principles outlined in California Education Code §33328.5, ensuring that any AI systems used in connection with the Service align with values of equity, safety, transparency, and accountability in the interest of student welfare.
- 1.2.** Sub-licensing Student Data for such purposes is strictly prohibited unless explicit written permission is obtained from the student's parent, legal guardian, or eligible student.
- 1.3.** Ownership of all Student Data, including content generated with AI assistance, remains with the District or the student, as applicable.

2. Notification and Consent

- 2.1.** If any feature of the Service is modified to include AI functionality (or if a non-AI provider intends to introduce AI features), the Provider shall notify the District in writing prior to deployment.
- 2.2.** The Provider must disclose the specific AI architecture (including third-party tools used), the purpose of such use, and how Student Data will be processed within these features.
- 2.3.** No AI feature may be enabled until the District provides written consent and has reviewed any updated data-handling practices.

3. Algorithm Bias and Fairness

- 3.1.** The Provider certifies that any AI technologies used in facilitating the Services (whether proprietary or integrated via third parties) are regularly audited for algorithmic bias and fairness.
- 3.2.** Upon request by the District, the Provider shall furnish a summary of audit findings related to bias detection and mitigation strategies. For third-party embedded AI, providing official third-party audit reports or compliance attestations shall satisfy this requirement. These audits shall demonstrate commitment to promoting equitable outcomes and addressing systemic bias under California Education Code §33328.5(d).

4. AI Hallucinations and Reliability

- 4.1.** The Provider shall monitor the hallucination rate of any deployed generative AI models (e.g., large language models or chatbots) and employ industry-standard techniques to reduce the occurrence of inaccurate or misleading outputs.

4.2. The Provider shall maintain a mechanism for the District to report hallucinated or harmful responses and address such issues in a timely and accountable manner

5. Prohibited Uses of AI

The Provider shall not (and shall ensure its sub-processors do not):

- 5.1.** Use AI to generate synthetic or inferred Student Data.
- 5.2.** Develop behavioral profiles for marketing or advertising.
- 5.3.** Engage in predictive analytics that may result in automated decision-making affecting students without human oversight.
- 5.4.** Deploy AI systems that are not designed to minimize harmful outcomes to minors, including but not limited to biased academic profiling or discriminatory content outputs.

These prohibitions align with California Education Code §33328.5(c), which calls for educational AI technologies to be designed to minimize harm and safeguard the well-being of students.

6. Student Content and AI-Generated Work

If students create content using AI tools embedded in the Service (e.g., essays, responses, or projects), the Provider shall:

- 6.1.** Ensure students can download or export that content.
- 6.2.** Retain no ownership or claim over AI-assisted student work.
- 6.3.** Maintain logs of AI interactions in accordance with FERPA.
- 6.4.** Support digital literacy and public awareness regarding the use of AI, in accordance with §33328.5(b), by enabling users to understand when they are interacting with an AI system.

7. Transparency and Disclosure Requirements (SB 942)

7.1. To the extent required by California SB 942, the Provider shall maintain and make available tools or mechanisms to verify whether content was generated by AI, including provenance data where applicable. This tool shall:

- 7.1.1.** Provide provenance data (excluding personal data).
- 7.1.2.** Support multiple content formats.
- 7.1.3.** Accept user feedback to support continuous improvement.

7.2. All AI-generated content must include latent disclosures that identify:

- 7.2.1.** The Provider's name.
- 7.2.2.** Identification of the AI system used.
- 7.2.3.** The creation date and time.
- 7.2.4.** A unique identifier for the generated content.

7.3. The Provider shall also offer users the option to include visible disclosures indicating that the content was generated by AI. These disclosures must be conspicuous and designed to resist removal.

7.4. If the Provider licenses its AI technology to third parties, such license agreements shall require those third parties to uphold the same transparency and disclosure standards outlined herein.

8. Third-Party AI Sub-processors & Embedded Tools

8.1. Flow-Down Obligations: If the Provider embeds, integrates, or queries third-party AI models or APIs (e.g., OpenAI, Anthropic, Azure OpenAI), the Provider remains fully responsible for ensuring such third parties comply with the privacy, non-training, and security standards set forth in this Addendum.

8.2. Zero-Data Retention / No Training Guarantee: The Provider certifies that all third-party AI integrations operate under enterprise API agreements that strictly prohibit the third-party AI vendor from retaining, logging, or using Student Data to train their underlying models.

8.3. Exemptions for Standard Third-Party Infrastructure: Where the Provider leverages external foundation models, compliance with Sections 3 (Auditing) and 7 (Provenance) may be fulfilled by providing the underlying vendor's published safety, transparency, and audit documentation.

9. Definitions

9.1. Artificial Intelligence (AI): Systems that analyze data and take actions, with some degree of autonomy, to achieve specific goals.

9.2. Hallucination: A response generated by an AI system that is incorrect, nonsensical, or misleading while appearing factually accurate.

9.3. Algorithmic Bias: Systematic and unfair discrimination in outcomes generated by an algorithm based on characteristics such as race, gender, or disability.

10. Compliance with State Advisory Guidelines

10.1. The Provider shall monitor and cooperate with any guidance or recommendations issued by the California Department of Education's Artificial Intelligence in Education Advisory Council, as established under Education Code §33328.5(a). This cooperation may include participation in feedback initiatives, alignment with recommended practices, or revisions to data governance protocols in response to evolving regulatory requirements.

Service Provider Signature

Kimberly A. Johnson

Date Signed

10/20/2026 09:35 am

DATA INCIDENT NOTIFICATION ADDENDUM

This Exhibit outlines the Vendor's obligations in the event of a Data Incident involving Customer Data. These obligations are in addition to and do not limit any rights or remedies available to the Customer under the Agreement or applicable law.

1. Data Incident Notification

1.1. In the event Roseville City School District ("RCSD" or "District" or "Customer") Data is accessed, acquired, or reasonably believed to have been accessed or acquired by an unauthorized individual or third party ("Data Incident"), the Vendor shall notify the Customer in writing without undue delay, and in no case later than seventy-two (72) hours after confirming the occurrence of the Data Incident.

1.2. The Vendor shall comply with all reasonable instructions from the District in relation to the Data Incident and, in consultation with the District, take all appropriate and reasonable steps to investigate and mitigate any known or anticipated harmful effects resulting from such unauthorized access, use, or disclosure of Customer Data.

1.3. If the Data Incident involves Personally Identifiable Data (PII), including but not limited to Social Security numbers, government-issued identification numbers, financial account details, health records, or medical information protected under applicable privacy laws (e.g., HIPAA, FERPA, CCPA, SOPIPA, GDPR, CRPA, etc), the Vendor shall apply heightened protections in accordance with applicable state and federal law, including but not limited to breach notification, identity theft prevention, and mitigation requirements.

2. Notification to Affected Individuals and Authorities

The obligations in this Section apply in all cases where the Data Incident is caused, in whole or in part, by the actions or omissions of the Vendor, its subcontractors, or affiliates.

2.1. Following confirmation of a Data Incident, the vendor shall provide written notification to affected individuals whose data was compromised. This notification shall:

2.1.1. Be written in plain language;

2.1.2. Be delivered in compliance with applicable federal, state, or provincial laws;

2.1.3. Be issued without unreasonable delay following the District's approval and any required consultation with law enforcement

2.2. The notification to affected individuals shall include, at a minimum:

2.2.1. A general description of the incident and the Vendor's response efforts.

2.2.2. The contact information of the Vendor's designated incident response representative.

2.2.3. The type(s) of Customer Data or PII involved (e.g., name, address, date of birth, Social Security number, student records, health/medical information, etc.);

2.2.4. The known or estimated date(s) of the Data Incident and the date of notification.

2.2.5. Whether law enforcement was involved and whether any delay in notification was due to a law enforcement investigation.

2.2.6. Steps the individual can take to protect themselves.

2.3. The Vendor agrees to adhere to all applicable federal, state, and provincial laws concerning the protection of Customer Data, including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA), where applicable.

In the event of a Data Incident involving Personally Identifiable Information (PII) of a minor, the Vendor acknowledges that PII includes both direct and indirect identifiers that could reasonably identify an individual student. Under FERPA, PII includes, but is not limited to:

- Student's full name
- Student identification number or state/local student identifier
- Date and/or place of birth
- Grade level or classroom assignment
- School name or teacher name
- Mailing address or contact information
- Parent/guardian names and contact information
- Any combination of the above elements that would reasonably allow identification of the student with reasonable certainty

2.4. If such PII is involved in a Data Incident, the Vendor shall:

2.4.1. The Vendor shall fully fund and coordinate identity monitoring and/or credit monitoring services for a minimum of twelve (12) months, including, at a minimum, dark web monitoring, identity theft insurance, and access to fraud resolution agents, without cost to the affected individual or the District.

2.4.2. As described in Section 2.2, notify all affected individuals (or their legal guardians, as applicable).

2.4.3. If five hundred (500) or more individuals are affected, the Vendor shall notify the appropriate State Attorney General or supervisory authority in accordance with relevant state data breach laws and ensure that the notification complies with all timing, format, and content requirements set forth under the relevant state's breach notification statute. A copy of the regulatory notification shall be provided to the Customer.

2.4.4. Maintain a record of the Data Incident, including the nature of the breach, categories of data affected, notification steps taken, and services provided. Upon request, the customer will have access to these records.

2.4.5. The Vendor shall ensure that all breach response and notification processes are consistent with applicable FERPA guidance and any other relevant federal, state, or provincial privacy regulations. No PII shall be re-disclosed or shared with any third party, including subcontractors or affiliated entities, without prior written consent from the District or as explicitly required by law. The Vendor shall document and maintain detailed records of all data disclosures related to the incident and shall make those records available to the District upon request.

3. Legal Compliance and Risk Management

The Vendor agrees to comply with all applicable local, state, provincial, and federal data privacy and security laws, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)

State-specific data breach notification statutes

3.1. The Vendor shall maintain a written incident response and breach notification policy that complies with industry standards and applicable law. The Vendor shall, upon request, make a summary of its policy available to the District.

3.1.1. The Vendor shall ensure that any subcontractor, service provider, or third party with access to Customer Data is contractually bound by equivalent or stronger data protection, confidentiality, and incident response obligations as outlined in this Agreement. The Vendor shall remain fully responsible for any acts or omissions of such third parties in connection with the handling of Customer Data.

3.2. At the District's request, and where such assistance is not unduly burdensome, the Vendor shall provide reasonable cooperation and support for any investigation, regulatory inquiry, or litigation arising out of or relating to the Data Incident, including support in notifying affected individuals and interfacing with regulatory authorities.

3.3. The Vendor shall not disclose the existence or details of a Data Incident to any third party, including media, regulators, or other customers, without the District's prior written approval, except as strictly required by law.

3.4. In no event shall the District be held financially liable for any costs, damages, regulatory penalties, or legal expenses arising from a breach of Customer Data caused, in whole or in part, by the Vendor, its subcontractors, or affiliates. The Vendor shall be solely responsible for all costs associated with investigation, response, notification, remediation, credit or identity monitoring, and any regulatory or legal actions stemming from such a breach.

3.5. The Vendor shall fully indemnify, defend, and hold harmless the District from and against any and all claims, damages, liabilities, penalties, costs, and expenses (including reasonable attorneys' fees) arising from or related to a Data Incident caused, in whole or in part, by the Vendor, its subcontractors, or agents. This includes, but is not limited to, costs associated with breach notification, regulatory inquiries, litigation, and third-party claims.

Service Provider Signature

Date Signed

Kimberly A. Johnson

10/20/2026 09:43 am

This Agreement constitutes the entire understanding among the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral. No amendment or modification of this Agreement shall be valid unless in writing and signed by authorized representatives of both Parties.

As an authorized representative of my organization, I accept the conditions listed in this document.

Authorized Representative Signature

Date

Kimberly A. Johnson

10/21/2026 09:51 am

Service Provider

Roseville City School District

Date

10/20/2026 09:43 am

Service Provider

Name

Kimberly A. Johnson

Service Provider

Title

Sr. VP Business Operations

Service Provider

Email (Service Provider)

contracts@teachtown.com

Service Provider

Name

Laura Assem

Roseville City School District

Title

Executive Director, Technology

Roseville City School District

TeachTown Accessibility Conformance Report

Remediation Plan (Last Updated March 2026)

(Based on WCAG 2.1)

WCAG 2.1 Roadmap

Criteria	Conformance Level	Remarks and Explanations
2.1.1 Keyboard (Level A)	Plan: Move Admin to Supports	Admin Updates Planned for Table Navigation in Q1 2027.
2.5.1 Pointer Gestures (Level A 2.1 only)	Plan: Additional lessons in Supports	Additional scannable lessons and options on roadmap for late 2026 and 2027.
4.1.2 Name, Role, Value (Level A)	Plan: Move to Supports	Updates to move to support planned for Q3 2026.
1.4.3 Contrast (Minimum) (Level AA)	Plan: Move to Supports	Updates planned in Q3 2026.

TeachTown Accessibility Conformance Report

International Edition

(Based on WCAG 2.1)

Name of Product/Version:

TeachTown website for enCORE

Report Date:

March 2026

Product Description:

TeachTown Inc. maintains one Product Site:

- www.teachtown.com. Providing web-based applications and learning management functions to our customers. All access to this site requires login credentials.

Contact Information:

productfeedback@teachtown.com

Notes:

All TeachTown products are web-based, and function with HTML5-compliant browsers. Our product technology platform is HTML5. The Conformance Level for each item in the included Standards are evaluated on the basis of the ability of our platform to support the item. Not every piece of content that is presented on our web site, or within our web applications, may fully implement an item.

Evaluation Methods Used:

Testing is based on knowledge of general product functionality along with 3rd party tools/readers to validate accessibility.

Applicable Standards/Guidelines

This report covers the degree of conformance for the following accessibility standard/guidelines for enCORE:

Standard/Guideline	Included In Report
Web Content Accessibility Guidelines 2.1	Level A (Yes) Level AA (Yes) Level AAA (No)

Terms

The terms used in the Conformance Level information are defined as follows:

- **Supports:** The functionality of the product has at least one method that meets the criterion without known defects or meets with equivalent facilitation.
- **Partially Supports:** Some functionality of the product meets the criterion without known defects but not all areas meet 100% of the criterion.
- **Does Not Support:** The majority of product functionality does not meet the criterion.
- **Not Applicable:** The criterion is not relevant to the product.
- **Not Evaluated:** The product has not been evaluated against the criterion.

WCAG 2.1 Report

Note: When reporting on conformance with the WCAG 2.1 Success Criteria, they are scoped for full pages, complete processes, and accessibility-supported ways of using technology as documented [here](#)

Table 1: Success Criteria, Level A

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.1.1 Non-text Content (Level A)	Web: Supports	Fully supported via HTML5, however not all instances on non-text content may fully implement this subject to Learning Content design criteria.
1.2.1 Audio-only and Video-only (Prerecorded) (Level A)	Web: Supports	Fully supported via HTML5
1.2.2 Captions (Prerecorded) (Level A)	Web: Supports	Fully supported via HTML5 using the video tag with accompanying text and time markers
1.2.3 Audio Description or Media Alternative (Prerecorded) (Level A)	Web: Supports	Fully supported via HTML5
1.3.1 Info and Relationships (Level A)	Web: Supports	Fully supported via HTML5
1.3.2 Meaningful Sequence (Level A)	Web: Supports	Via custom HTML5 attributes
1.3.3 Sensory Characteristics (Level A)	Web: Supports	Fully supported via HTML5
1.4.1 Use of Color (Level A)	Web: Supports	Aspects of lessons that are specifically teaching color may be an exception.
1.4.2 Audio Control (Level A)	Web: Supports	All audio used in student lessons is leveled for consistency. Educators can control overall volume levels.
2.1.1 Keyboard (Level A)	Web: Partially Supports	Special accessibility devices may be employed for students that cannot operate a mouse. Worksheets are provided in printed form. Admin updates are planned for Table navigation.
2.1.2 No Keyboard Trap (Level A)	Web: Supports	Support may vary based on type of student lesson by design based on curriculum use.
2.1.4 Character Key Shortcuts (Level A 2.1 only)	Web: Not Applicable	Does not apply with the exception of switch scanning that does employ a single key
2.2.1 Timing Adjustable (Level A)	Web: Supports	For our purposes this applies mostly to the configuration of student lesson content. Educators are provided various adjustment controls where applicable.

2.2.2 Pause, Stop, Hide (Level A)	Web: Supports	Only provided in situations where this is appropriate for student lesson content.
2.3.1 Three Flashes or Below Threshold (Level A)	Web: Supports	
2.4.1 Bypass Blocks (Level A)	Web: Supports	
2.4.2 Page Titled (Level A)	Web: Supports	Interactive student lessons may not be titled.
2.4.3 Focus Order (Level A)	Web: Supports	
2.4.4 Link Purpose (In Context) (Level A)	Web: Supports	Precise implementation varies based on UX design requirements.
2.5.1 Pointer Gestures (Level A 2.1 only)	Web: Supports	Scannable lesson options with full support.
2.5.2 Pointer Cancellation (Level A 2.1 only)	Web: Supports	Student sessions are timed and intentional exceptions
2.5.3 Label in Name (Level A 2.1 only)	Web: Supports	
2.5.4 Motion Actuation (Level A 2.1 only)	Web: Not Applicable	
3.1.1 Language of Page (Level A)	Web: Supports	TeachTown site is currently English only and only sold in North America. Some student lessons are available for the student in Spanish as English Language Learners.
3.2.1 On Focus (Level A)	Web: Supports	In no case is the on focus event used to modify HTML content.
3.2.2 On Input (Level A)	Web: Supports	
3.3.1 Error Identification (Level A)	Web: Supports	An exception is that many interactive student lessons are designed as tests and deliberately do not provide error identification feedback.
3.3.2 Labels or Instructions (Level A)	Web: Supports	Precise implementation varies based on UX design requirements.
4.1.1 Parsing (Level A)	Web: Supports	All HTML5 content is "well formed".
4.1.2 Name, Role, Value (Level A)	Web: Partially Supports	Standard HTML controls are used almost exclusively, so as per the guideline this is arguably inapplicable.

Table 2: Success Criteria, Level AA

Notes:

Criteria	Conformance Level	Remarks and Explanations
1.2.4 Captions (Live) (Level AA)	Web: Supports	HTML5 supports live captions separate from the audio itself. But this is not always appropriate to our lesson content.
1.2.5 Audio Description (Prerecorded) (Level AA)	Web: Supports	HTML5 supports live captions separate from the video itself. But this is not always appropriate to our lesson content.
1.3.4 Orientation (Level AA 2.1 only)	Web: Supports	
1.3.5 Identify Input Purpose (Level AA 2.1 only)	Web: Supports	
1.4.3 Contrast (Minimum) (Level AA)	Web: Partially Supports	Lowest contrast ratio is 7:1 in website. Certain lesson content has specific color guidelines.
1.4.4 Resize text (Level AA)	Web: Supports	For certain lesson content may not be permitted for layout and UX concerns.
1.4.5 Images of Text (Level AA)	Web: Supports	For certain lesson content images of text are used to specific effect. However in most cases text is used.
1.4.10 Reflow (Level AA 2.1 only)	Web: Supports	Student sessions intentionally do not allow this during trials
1.4.11 Non-text Contrast (Level AA 2.1 only)	Web: Supports	
1.4.12 Text Spacing (Level AA 2.1 only)	Web: Supports	Intentional exceptions in student sessions
1.4.13 Content on Hover or Focus (Level AA 2.1 only)	Web: Supports	
2.4.5 Multiple Ways (Level AA)	Web: Supports	All student lesson content requires views be accessed in a particular order. Wherever possible, other web pages such as in our customer-facing management tools, multiple ways of accessing are provided.
2.4.6 Headings and Labels (Level AA)	Web: Supports	
2.4.7 Focus Visible (Level AA)	Web: Supports	
3.1.2 Language of Parts (Level AA)	Web: Supports	Typically the local code is always available for programmatic detection. However, currently the TeachTown website is English only, sold only in North America.
3.2.3 Consistent Navigation (Level AA)	Web: Supports	Generally always true. We continually strive for UX design improvements.
3.2.4 Consistent Identification (Level AA)	Web: Supports	Generally always true. We continually strive for UX design improvements.
3.3.3 Error Suggestion (Level AA)	Web: Supports	Error descriptions are provided wherever possible for users performing data entry or configuration. In the case of student lesson content, some are

		designed as test and do provide error feedback by design.
3.3.4 Error Prevention (Legal, Financial, Data) (Level AA)	Web: Supports	
4.1.3 Status Messages (Level AA 2.1 only)	Web: Supports	



System and Organization Controls 2 (SOC 2) Type 2 Report – SOC for Service Organizations: Trust Services Criteria

Report on TeachTown, Inc.'s Description of its Suite of Special Education Software Solutions and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security Throughout the Period April 1, 2023 to September 30, 2023

Bonadio & Co., LLP
Certified Public Accountants

REPORT ON TEACHTOWN, INC.'S DESCRIPTION OF ITS SUITE OF SPECIAL EDUCATION SOFTWARE SOLUTIONS AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY THROUGHOUT THE PERIOD APRIL 1, 2023 TO SEPTEMBER 30, 2023

Table of Contents

SECTION ONE.....	3
Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to <i>Security</i> and Other Information Not Covered by the Service Auditor's Report.....	4
SECTION TWO.....	8
Assertion of the Management of TeachTown, Inc.....	9
SECTION THREE.....	11
Management's Description of TeachTown, Inc.'s Suite of Special Education Software Solutions Throughout the Period April 1, 2023 to September 30, 2023.....	11
Introduction.....	12
Company Background.....	12
Services Provided.....	12
Scope of this Report.....	12
Principal Service Commitments and System Requirements.....	12
Components of the System Used to Provide the Services.....	14
Infrastructure.....	14
Software.....	15
People.....	16
Data.....	16
Processes and Procedures.....	18
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring.....	19
Control Environment.....	19
Risk Assessment Process.....	20
Information and Communication Systems.....	21
Monitoring Controls.....	21
Changes to the System During the Period.....	21
Trust Services Categories, Criteria, and Related Controls.....	22
Complementary User Entity Control Considerations.....	23
Complementary Subservice Organization Control Considerations.....	24
SECTION FOUR.....	26
Trust Services Categories, Criteria, Related Controls, and Tests of Controls.....	27
SECTION FIVE.....	64
Other Information Provided by TeachTown, Inc. That is Not Covered by the Service Auditor's Report.....	65
Management's Response to Control Exceptions.....	65

SECTION ONE

**Independent Service Auditor's Report on a Description of a Service
Organization's System and the Suitability of the Design and Operating
Effectiveness of Controls Relevant to Security and Other Information Not
Covered by the Service Auditor's Report**

**INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION
OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY
OF THE DESIGN AND OPERATING EFFECTIVENESS OF
CONTROLS RELEVANT TO SECURITY AND OTHER INFORMATION
NOT COVERED BY THE SERVICE AUDITOR'S REPORT**

To: Management of TeachTown, Inc.

Scope

We have examined TeachTown, Inc.'s accompanying description of its Suite of Special Education Software Solutions found in Section 3 titled "Management's Description of TeachTown, Inc.'s Suite of Special Education Software Solutions Throughout the Period April 1, 2023 to September 30, 2023" (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TeachTown, Inc., to achieve TeachTown, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents TeachTown, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TeachTown, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

TeachTown, Inc. uses subservice organizations to provide hosting, managed network and security, and information technology support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TeachTown, Inc., to achieve TeachTown, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents TeachTown, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TeachTown, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY AND OTHER INFORMATION NOT COVERED BY THE SERVICE AUDITOR'S REPORT (CONTINUED)

Scope (Continued)

The information included in Section 5 titled "Other Information Provided by TeachTown, Inc. That is Not Covered by the Service Auditor's Report," is presented by TeachTown, Inc.'s management to provide additional information and is not a part of TeachTown, Inc.'s description of its Suite of Special Education Software Solutions made available to user entities during the period April 1, 2023 to September 30, 2023. Information about TeachTown, Inc.'s management responses to control exceptions identified in Section 4 of the report has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Service Organization's Responsibilities

TeachTown, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements were achieved. In Section 2, TeachTown, Inc. has provided the accompanying assertion titled "Assertion of the Management of TeachTown Inc.," (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. TeachTown, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY AND OTHER INFORMATION NOT COVERED BY THE SERVICE AUDITOR'S REPORT (CONTINUED)

Service Auditor's Responsibilities (Continued)

- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report.

Opinion

In our opinion, in all material respects—

- a. the description presents TeachTown, Inc.'s Suite of Special Education Software Solutions that was designed and implemented throughout the period April 1, 2023 to September 30, 2023 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of TeachTown, Inc.'s controls throughout that period.

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY AND OTHER INFORMATION NOT COVERED BY THE SERVICE AUDITOR'S REPORT (CONTINUED)

Opinion (Continued)

- c. the controls stated in the description operated effectively throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TeachTown, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of TeachTown, Inc.; user entities of TeachTown, Inc.'s Suite of Special Education Software Solutions during some or all of the period April 1, 2023 to September 30, 2023, business partners of TeachTown, Inc. subject to risks arising from interactions with the Suite of Special Education Software Solutions, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

Amherst, New York

January 4, 2024

SECTION TWO

Assertion of the Management of TeachTown Inc.

ASSERTION OF THE MANAGEMENT OF TEACHTOWN, INC.

January 4, 2024

We have prepared the accompanying description of TeachTown, Inc.'s Suite of Special Education Software Solutions titled "Management's Description of TeachTown, Inc.'s Suite of Special Education Software Solutions Throughout the Period April 1, 2023 to September 30, 2023" (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Suite of Special Education Software Solutions that may be useful when assessing the risks arising from interactions with TeachTown, Inc.'s system, particularly information about system controls that TeachTown, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

TeachTown, Inc. uses subservice organizations to provide hosting, managed network and security, and information technology support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TeachTown, Inc., to achieve TeachTown, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents TeachTown, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TeachTown, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TeachTown, Inc., to achieve TeachTown, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

- 1) The description presents TeachTown, Inc.'s Suite of Special Education Software Solutions that was designed and implemented throughout the period April 1, 2023 to September 30, 2023 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of TeachTown, Inc.'s controls throughout that period.

ASSERTION OF THE MANAGEMENT OF TEACHTOWN, INC. (CONTINUED)

- 3) The controls stated in the description operated effectively throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that TeachTown, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TeachTown, Inc.'s controls operated effectively throughout that period.

Brad Sheneman

Director of Technology

Margaret Lawless

Chief Product Officer

SECTION THREE

**Management's Description of TeachTown, Inc.'s Suite of Special Education
Software Solutions Throughout the Period April 1, 2023 to September 30,
2023**

INTRODUCTION

Company Background

TeachTown, Inc. (TeachTown or the Company), a division of Jigsaw Learning, Inc., was established in 2023. TeachTown is a remote entity with an office/warehouse located in Woburn, MA. TeachTown operates in North America, relying on around 100 full-time employees and also leveraging on-demand talent.

TeachTown's mission is to measurably improve the academic, behavioral, and adaptive functioning of students with disabilities. Per the Company's vision statement, "All children with disabilities will acquire & maintain the academic, social & emotional, and adaptive skills necessary to succeed."

Services Provided

TeachTown provides special education services to school districts and serves districts by providing core curriculum and intervention products for special education. The Company's services include full curriculum, a technical platform for curriculum use and supporting technical and professional services.

The Company has around 3,000 district customers and serves over 200,000 students. TeachTown also has a small number of parents that purchase TeachTown services directly.

Scope of this Report

This report describes TeachTown's internal controls related to the processing of user entity transactions within the Suite of Special Education Software Solutions throughout the period April 1, 2023 to September 30, 2023 and is intended to provide reasonable assurance as to the presence of controls relating to the security category included in the 2017 AICPA Trust Services Criteria (TSC) and information to interested parties so that they may better understand TeachTown's controls as they relate to their use of the solutions.

Although the descriptions in this report are comprehensive, they do not encompass all aspects of services provided or procedures followed by TeachTown.

Principal Service Commitments and System Requirements

TeachTown designs its processes and procedures to meet its objectives for its Special Education Software. Those objectives are based on the service commitments that TeachTown makes to user entities, the applicable laws and regulations that govern the Special Education Software, and the financial, operational, and compliance requirements that TeachTown has established for the services. Security commitments to user entities are documented and communicated in customer agreements. Security commitments are aligned to the National Institute of Standards & Technology Cybersecurity Framework ("NIST CSF") and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Special Education Software that are designed to permit system users to access the information they need based on their role in the system, while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

INTRODUCTION (CONTINUED)

Principal Service Commitments and System Requirements (Continued)

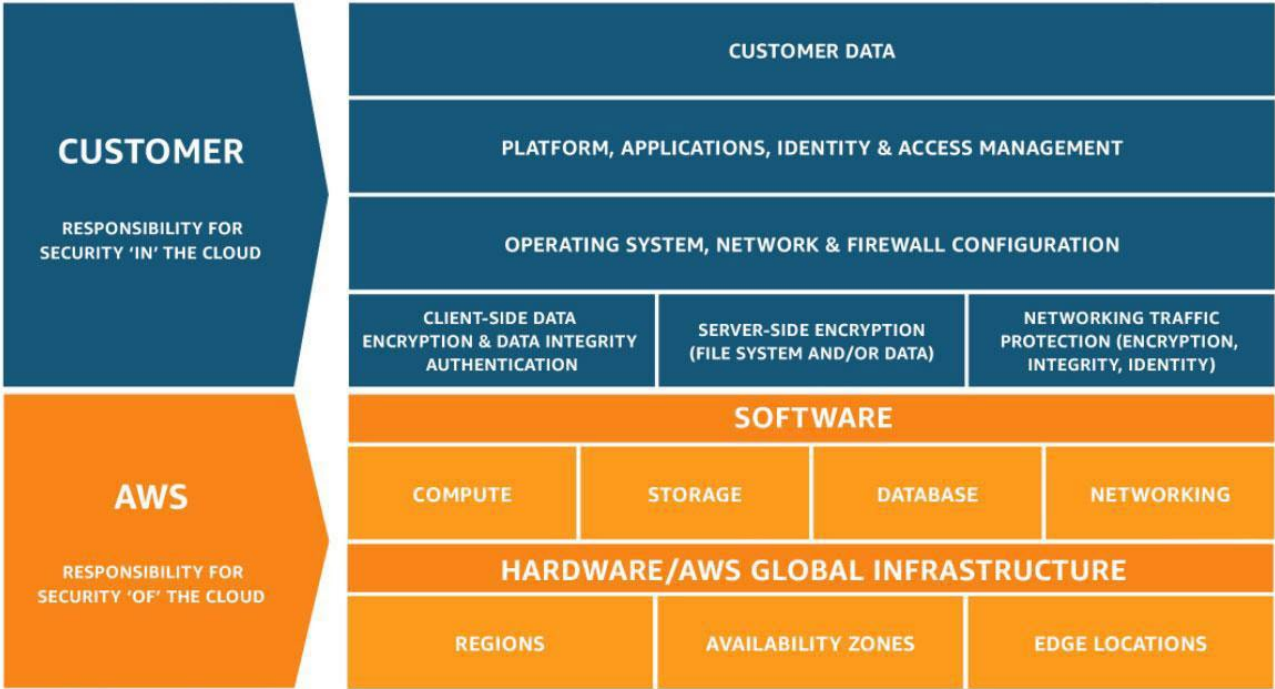
TeachTown establishes operational requirements that support the achievement of security commitments, applicable laws and regulations, and other system requirements. Such requirements are communicated in TeachTown's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required for the operation and development of the Special Education Software.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

Infrastructure

The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

TeachTown’s production application and related infrastructure reside in Amazon Web Services (AWS). All facilities, servers, storage, environmental monitoring equipment, data storage devices and media, internal networks and connected external telecommunications networks are deployed and managed by AWS staff in accordance with the AWS Shared Responsibility Model as shown below.



Customer data is hosted in AWS data centers located in the United States. AWS does not permit non-employees access to their data center facilities. Logical access is restricted using industry best practices for hosting applications with public cloud service providers. AWS physical security controls include, but are not limited to, perimeter controls, such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. AWS authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television cameras (CCTV) as defined in the AWS Data Center Physical Security Policy. AWS’ annual SOC 2 Type 2 attestation reports provide additional details on the specific control activities executed by the third-party. Additionally, AWS has been validated and certified by an independent service auditor to be in compliance with the ISO 27001 certification standard.

As a tenant of AWS, TeachTown naturally adopts the usage of the third-party’s proprietary overlay protocol utilized when systems in its environment need to communicate with each other via public networks. Data sent over these networks is encrypted. Data is encrypted at rest and in motion.

Within the AWS environment, TeachTown leverages AWS Elastic Compute Cloud (EC2) virtual machines for compute, AWS Elastic Block Store (EBS) for storage, and AWS Virtual Private Cloud (VPC) for logical network isolation.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

Infrastructure (Continued)

Infrastructure administration is performed via the AWS Management Console; a web application that leverages transport layer security (TLS) standards and protocols to protect administrative traffic in transit. The AWS Management Console is available at the following uniform resource locator (URL):

- <https://console.aws.amazon.com/>

Software

The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

TeachTown software products are software-as-a-service (SaaS) applications hosted by AWS in the United States and are available 24/7. A supported web browser and an Internet connection are required to access TeachTown products. TeachTown employees perform the initial provisioning based on customer programs including their staff logins (i.e., administrators, teachers, etc.). Account activation occurs at the start of the TeachTown subscription date.

In addition to the basic configurations, single sign-on (SSO) via Security Assertion Markup Language (SAML) can be set up. TeachTown also has integrations with other student information services, including OneRoster and ClassLink.

The TeachTown production application runs on the Windows server operating system. Data is stored in a Microsoft Structured Query Language (SQL) Server database. The application, developed using Microsoft technologies, is available via the web at the following URL:

- <https://www.teachtown.com/login.aspx>

TeachTown also maintains a series of mobile applications on the iTunes app store for iPads users only. Those applications include:

- enCORE High School
- enCORE Middle School
- TeachTown enCORE
- Student Lesson Plans (SLP) Assist
- TeachTown Transition
- Meta-Play
- TeachTown BE SAFE
- TeachTown Basics
- TeachTown Social Skills

The iPad applications are available at the following URL:

- <https://apps.apple.com/us/developer/teachtown-a-division-of-jigsaw-learning-inc/id899310519?see-all=i-pad-apps>

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

People

The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

The governance, risk, compliance, and privacy of TeachTown's production application rolls up to the Chief Product Officer (CPO). The CPO delegates security and privacy responsibilities to a group of full-time employees that includes the Chief Technology Officer (CTO), Information Technology (IT) Director, and Software Architect.

TeachTown also leverages On Demand Talent (ODT) to augment its full-time employees. The ODT includes:

- A Virtual Chief Information Security Officer (vCISO), a Security Consultant, and Privacy Experts from SideChannel.
- IT support from Electric.ai, a managed services provider (MSP).
- Managed security services provider (MSSP) support from High Wire Networks.

Data

The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system.

When TeachTown provides its service to an educational institution or parent, the Company collects personal information that is directly related to an identifiable student. A Privacy Notice is in place that refers to that type of information as "Student Data." TeachTown considers Student Data to be confidential and does not use Student Data for any purpose other than to provide its service on behalf of an educational institution or parent and in accordance with any contractual agreements between TeachTown and the educational institution or parent.

Access to data (i.e., student, teacher, school, etc.) stored in the application requires a valid user account, username and password, and is limited to the application user. An authorized user with the appropriate user permissions can create user accounts. All users are required to initiate a valid session, which expires after sixty (60) minutes of inactivity. All sign-ins by users authorized to view application data are logged with a timestamp, account identification (ID), and Internet Protocol (IP) address. Any pages that require a user to enter their account information are encrypted using TLS. All passwords are stored in the database in an encrypted format created with a one-way hash.

The Company uses a client-server model, which is structured to partition tasks or workloads between TeachTown's resources and services and its clients. Industry standard TLS 1.2 Advanced Encryption Standard 256 (AES-256) encryption is used by TeachTown for all client-server interactions.

TeachTown utilizes virtual desktop interfaces to securely access data in its environments. As such, no data leaves the cloud environment. Additionally, TeachTown's non-production environment utilizes the same controls as noted above.

The Company utilizes an enterprise grade anti-malware/anti-virus capability that provides file integrity monitoring for systems in its environment. This capability naturally provides detections needed to respond to possible incidents. In accordance with least privilege principles, access to audit logs are restricted to authorized personnel. TeachTown has identified auditable event/log categories across its systems. As such, system owners have configured these systems to record continuously the security-related events in accordance with Company requirements. Logs are monitored by High Wire Networks' Security Operations Center personnel and anomalous activity is alerted appropriately for review and analysis.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

Data (Continued)

TeachTown utilizes several mandatory technical controls for workstations in its environment. Some examples include: host based firewall with strict port/protocols limitations, anti-virus/anti-malware, endpoint detection and response (EDR), and patch management. Similarly, the Company utilizes the same mandatory technical controls within its server environment, with some notable additions including: hardened images in alignment with industry recognized authoritative sources on configuration management, network based firewall, and vulnerability scanning. A Web Application Firewall (WAF) and network-based firewall are in place to protect Company systems from unauthorized access.

As a tenant of AWS, TeachTown relies on the third-party's controls in regard to privilege access for administrative consoles. AWS states the following within their annual SOC 2 Type 2 attestation reports: "AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization."

TeachTown has a documented procedure outlining the steps taken to sanitize computing resources of tenant personally identifiable information when provided with a request from an individual or entity to do so. As a tenant of AWS, TeachTown relies upon industry recognized techniques (i.e., the National Institute of Standards and Technology (NIST) Special Publication 800-88: Guidelines for Media Sanitization) for decommissioning storage nodes that provide a level of assurance that customer data is not exposed to unauthorized individuals.

TeachTown maintains a comprehensive privacy program to address the data in which the Company collects, uses and discloses as a result of the operation of its online solution. The Company considers personal information, including Student Data, to be confidential and does not use Student Data for any purpose other than to provide the service on the client's behalf, in accordance with any contractual agreements with school districts and parents. TeachTown's collection, use, and disclosure of student data is in accordance with their Terms of Service and/or any other agreement with school districts and parents, and by the provisions of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and applicable state laws which relate to the collection, use, and disclosure of Student Data. TeachTown collects, maintains, uses, and shares Student Data only for an authorized educational purpose and as described in their agreements with school districts and parents, or as directed by their clients. Additional information on how TeachTown collects, processes, stores, and shares application data is documented in the Company's published Privacy Notice, which is available at the following URL:

- <https://web.teachtown.com/privacy-policy/>

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

Processes and Procedures

The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information are prepared.

TeachTown implements formal, documented policies and procedures that provide guidance for operations and information security within the Company. Each policy addresses a purpose, scope, ownership, roles, and responsibilities. Employees who violate TeachTown standards and/or protocols are investigated and appropriate disciplinary action (i.e., a warning, performance plan, suspension, and/or termination) is followed. TeachTown information security and privacy policies are reviewed and approved at least annually by leadership personnel.

The Company's incident response plan has been developed in alignment with several incident response related control objectives articulated in the NIST Cybersecurity Framework alongside NIST Special Publication 800-61 (Computer Security Incident Handling Guide).

Employees are provided training on how to recognize suspected security incidents and where to report them. TeachTown utilizes predefined and exclusive communication channels to enable its employees to report any potential incidents. For relationships with external entities, such parties are informed of their responsibility to report information security events through contractual agreements or contracts in place.

TeachTown restricts, logs, and monitors access to its information security systems, with support from High Wire Networks Security Operations Center personnel to monitor logs from these systems. Additionally, periodic access reviews take place and appropriate action to revoke or reduce privileges, where necessary, are executed based on the review.

Change management procedures are in place as the mechanism to document and approve access requests. Access is approved, granted and governed by logical access control policies configured in alignment with least privilege principles through the usage of AWS Identity and Access Management (IAM). As per the Company's offboarding standard operating procedure, access that is no longer required is revoked accordingly. Periodically, the standard operating procedure is audited to assess its operational effectiveness. A centralized directory service and IAM capability is used to manage and store the identity of all personnel who have access to the IT infrastructure.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Policies and procedures are formally documented to ensure that internal controls are met. On a monthly basis, Company-wide meetings are held. Key personnel presenting in these meetings discuss the state of the Company, key initiatives, and TeachTown's core values. Contractors are used by the Company when needed. Contractor workers are required to sign a contractor agreement prior to being employed by TeachTown. Vendor agreements must be in place before a third-party provides services to TeachTown. If the vendor has access to confidential information, such contracts should include appropriate privacy, confidentiality, and unauthorized disclosure reporting procedures and requirements. An Employment Handbook and Acceptable Use Policy (AUP) are in place that outline the Company's expectations that employees and contractors are to be informed on and follow. At hire, employees and contractors are required to sign an acknowledgement form stating they have read, understand and agree to the Employment Handbook and AUP.

A formal hiring process is in place to ensure candidates for employment are sufficiently interviewed and vetted. Background and reference checks are required prior to hiring. Once hired, employees are required to go through new hire training.

Employees and contractors must complete security and privacy training at hire and on an annual basis thereafter. The training covers the Company's policies and procedures, including how employees are to identify and report on security incidents.

An organizational chart is in place to ensure that the current roles and relationships between individuals within the Company have been established. The chart is updated as needed based on employment changes. Job descriptions are established for candidates for employment that define the open position's qualification, roles, and responsibilities requirements.

A Board of Directors is in place that meets on a quarterly basis. An agenda and meeting minutes are documented and maintained. The roles and responsibilities of Board members are documented, which state that the majority of Board members must be independent from management. Upon joining the Board, members are required to sign a Board agreement stating they have read, understand and agree to their roles and responsibilities. The agreement covers conflict of interest statements.

Other TeachTown teams that are in place to support the Company's control environment objectives include:

- An Executive Leadership Team that meets on a weekly basis to ensure Company goals and objectives are being met and monitored. An agenda and meeting minutes are documented and maintained.
- A Product Leadership Team that meets on a weekly basis to ensure the Company's information technology (IT), engineering and product objectives and timelines are being met and monitored. An agenda and meeting minutes are documented and maintained.
- An Information Security and Privacy Team that meets on a weekly basis to ensure the Company remains in compliance with its security and privacy requirements. An agenda and meeting minutes are documented and maintained.
- A Security Operations Center Team that meets on a bi-weekly basis to ensure the Company's operations are being met and monitored, and that operational updates are discussed. An agenda and meeting minutes are documented and maintained.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING (CONTINUED)

Risk Assessments Process

The following policies are in place to support the Company's risk identification, mitigation and management objectives:

- An Information Protection Policy is in place which outlines the classifications of the types of data in which the Company collects, and depending on that classification, how such data is to be handled.
- A Risk Management Policy is in place that outlines how the Company is to identify, assess, monitor, remediate, and report on newly identified and existing risks.
- A Vulnerability and Patch Management Policy is in place that outlines how the Company is to identify, evaluate, treat, and report on security vulnerabilities in systems and the software that runs on them.
- A Vendor Management Policy is in place that outlines how the Company is to select and manage external third-parties that the Company utilizes for support.
- A Change Management Policy is in place that defines the different levels of changes and the requirements that must be followed based on each type or risk.
- A Data Retention, Destruction, and Transfer Policy is in place which outlines how the Company is to securely maintain, handle and dispose of data and destroy old hardware.

On an annual basis, an independent third-party is contracted to perform a risk assessment of the Company's environment. The results are reviewed and corrective action plans are documented in a risk register. The potential for fraud is included as a part of the assessment performed.

External and credentialed vulnerability scans are conducted on a weekly basis using AWS provided vulnerability scanning technologies. Vulnerabilities are reviewed and remediated, as required. Remediation efforts are documented and maintained.

Vendor due diligence procedures are formally documented to ensure that the Company has appropriately evaluated the vendor's control objectives and commitments prior to contracting. On an annual basis, the Company requests and formally reviews assurance documentation from the applicable subservice organizations in-scope; including AWS, High Wire Networks, and Electric.ai.

Technical changes are tracked within the Company's ticketing system and the ticket must show a formal review, approval, and testing has been completed prior to the change being implemented. The changes must show through documentation that the segregation of duties was present. In addition, changes that are deemed major or significant by TeachTown require a backout plan to be established and agreed upon by all stakeholders and project team members.

Backups of data are performed to AWS on a daily basis and backup failure alerting has been configured. Per AWS' annual SOC 2 Type 2 attestation report, backups are encrypted. Administrative access to the backup information and settings are restricted to appropriate personnel as defined by TeachTown. In addition, data restoration testing is performed on a daily basis and testing procedures are documented and maintained.

Cyber liability insurance is in place and maintained.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING (CONTINUED)

Information and Communication Systems

As noted above, a suite of policies and procedures are in place to ensure employees and contractors are aware of their objectives and needed contribution to the Company's security and privacy obligations. On an annual basis, employee and contractor performance reviews take place. Such reviews are documented and maintained. Procedures are in place to ensure employee and contractor misconducts are handled and documented.

Email, Slack and Salesforce are utilized as the Company's main platforms for internal and external communication. Contact and service information is available on the Company's website for external parties. A Terms of Service and Privacy Notice are available on the Company's website. The Privacy Notice is clearly dated and describes how TeachTown collects, uses, and discloses personal information. When a user signs up for an account via TeachTown's website, as a part of the sign up process, they are required to acknowledge that they have read and agree to the End User License Agreement and the Facilitator Agreement. Within the Facilitator Agreement, a reference to the Company's Privacy Notice is included. Once an account has been successfully created, the user can access and modify their information as desired.

Monitoring Controls

In addition to the Company's monitoring controls defined above (i.e., vulnerability management, vendor management, etc.), endpoint protection is implemented and maintained on all laptops and workstations. Automatic updates are configured, real-time scanning is enabled, and full deep system scans are configured to be performed weekly. Administrative access to the solution is restricted to appropriate personnel as defined by TeachTown.

An Incident Response Plan is in place which outlines steps on how to detect, report, respond to, and recover from security incidents and breaches. The Company's Incident Response Plan is tested on an annual basis.

Access to the configuration of the AWS firewalls is restricted to appropriate personnel as defined by TeachTown. Firewall rules have been implemented to appropriately restrict network traffic.

The laptops and workstations in use are provided by the Company and a mobile device management tool is in place to inventory, monitor and manage such devices. The tool allows TeachTown to remotely wipe a device if it were to be reported lost or stolen.

Changes to the Solutions During the Period

There were no changes that are likely to affect report users' understanding of how TeachTown's Suite of Special Education Software Solutions are used to provide the services during the period from April 1, 2023 to September 30, 2023.

TRUST SERVICES CATEGORIES, CRITERIA, AND RELATED CONTROLS

Relevant trust services categories, criteria and related controls are included in Section 4 of this report, “Trust Services Categories, Criteria, Related Controls, and Tests of Controls,” to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the criteria and related controls are presented in Section 4, they are, nevertheless, an integral part of TeachTown, Inc’s description of its System.

COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS

TeachTown's services and controls were designed with the assumption that certain controls would be implemented by user entities (referred to as districts). In certain situations, the application of specific controls at user entities is necessary to achieve certain control objectives included in this report. There may be additional controls in operation at user entities to complement the control objectives identified in this report. In addition to those user control considerations, auditors of user entities should consider whether the following controls have been placed in operation at user entities:

TSC Associated	User Entity Control
CC2.1	User entities are responsible for the security and integrity of data housed at facilities under user entity control, particularly for data utilized by the Company's systems and services.
CC2.1 CC4.1 CC5.1 CC5.2	User entities are responsible for establishing, monitoring, and maintaining controls over the security for system generated outputs, and reports from the solutions.
CC5.3	User entities are responsible for implementing policies and procedures over the types of data that are allowed to be entered into the solutions.
CC6.1	User entities are responsible for reviewing access to their instance of the solutions periodically to evaluate appropriateness of access levels.
CC6.1 CC6.2 CC6.3	User entities are required to ensure unique user IDs and passwords are used to access system data.
CC6.1 CC6.7	User entities are responsible for sending data to the service organization via a secure connection and/or the data should be encrypted.
CC6.2 CC6.3	User entities are responsible for approving and creating new user access to the solutions.
CC6.2 CC6.3	User entities are responsible for removing terminated employees' access to the solutions.
CC7.3 CC7.4 CC7.5	User entities are responsible for notifying the service organization if they detect or suspect any security incident related to the solutions.
CC7.5	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or use the service organization's services.
CC8.1	User entities are responsible for reviewing email and other forms of communications from the service organization, related to changes that may affect the service organization's customers and users, and their security, confidentiality, or availability obligations.

The list of user entity control considerations presented above and those presented within certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROL CONSIDERATIONS

TeachTown's controls related to the Suite of Special Education Software Solutions cover only a portion of overall internal control for each user entity of the Company. It is not feasible for the control objectives related to services to be achieved solely by TeachTown. Therefore, each user entity's internal controls over TeachTown's Suite of Special Education Software Solutions must be evaluated in conjunction with the security controls and system requirements represented in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

The in-scope subservice organizations include:

- AWS
- Electric.ai
- High Wire Networks

TSC Associated	Subservice Organization Control
CC2.1	The subservice organizations are responsible for the completeness and accuracy of transaction processing on behalf of the service organization.
CC2.1	The subservice organizations are responsible for the completeness and accuracy of specified reports provided to and used by the service organization.
CC3.1 CC3.2 CC3.3 CC3.4 CC5.3 CC9.1 CC9.2	The subservice organizations are responsible for implementing a risk assessment policy and process to mitigate those risks that apply to their organizations.
CC4.1 CC4.2 CC5.1 CC5.2	The subservice organizations are responsible for monitoring internal control activities by having policies and procedures in place requiring the completion of periodic internal audits or quality control reviews.
CC6.1 CC6.2 CC6.3	The subservice organizations are responsible for implementing logical access controls relevant to the processing performed for the service organization.
CC6.4	The subservice organizations are responsible for implementing internal controls to ensure access to their servers that host the service organization's data is restricted, reviewed and managed on an ongoing basis.
CC7.3 CC7.4 CC7.5	The subservice organizations are responsible for implementing internal controls over the procedures to detect and respond to potential system incidents.
CC7.3 CC7.4 CC7.5	The subservice organizations are responsible for implementing a process to communicate significant system incidents and deviations in the effectiveness of the subservice organization's controls to service organization management.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROL CONSIDERATIONS (CONTINUED)

TSC Associated	Subservice Organization Control
CC8.1	The subservice organizations are responsible for implementing internal controls to ensure ongoing change and patch management occurs to limit the possibility of a security bug or incident.

The list of complementary subservice organization controls presented herein does not represent a comprehensive set of all controls performed by the subservice organizations. The list above notes controls which must be operating effectively within the subservice organizations to provide reasonable assurance that TeachTown's controls stated within Section 4 of this report are able to operate effectively.

SECTION FOUR

Trust Services Categories, Criteria, Related Controls, and Tests of Controls

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

(The 2017 AICPA Trust Services Criteria and TeachTown, Inc.'s related controls are included in this section, as well as the tests of controls and the results of the tests provided by Bonadio & Co., LLP.)

Applicable Trust Services Criteria Relevant to Security

Control Environment		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	TTI1.01 TTI1.02 TTI1.03 TTI1.04 TTI1.05
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	TTI1.06
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	TTI1.07 TTI1.08 TTI1.09 TTI1.10 TTI1.11 TTI1.12
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	TTI1.03 TTI1.05 TTI1.13 TTI1.14 TTI1.15
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	TTI1.03 TTI1.05 TTI1.06 TTI1.12 TTI1.15 TTI1.16

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Information and Communication		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	TTI2.01
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	TTI1.01 TTI1.02 TTI1.05 TTI1.06 TTI1.07 TTI1.08 TTI1.09 TTI1.10 TTI1.12 TTI1.14 TTI2.02
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	TTI1.03 TTI1.04 TTI2.01 TTI2.02 TTI2.03 TTI2.04 TTI2.05

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Risk Assessment		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	TTI3.01 TTI3.02 TTI3.03 TTI3.04
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	TTI3.05 TTI3.06 TTI3.07
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	TTI3.04 TTI3.05
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	TTI3.08 TTI3.09
Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	TTI3.06 TTI3.07 TTI4.01
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	TTI3.07

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Control Activities		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	TTI1.01 TTI3.01 TTI3.02 TTI3.03 TTI5.01 TTI5.02 TTI5.03
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	TTI1.01 TTI3.02 TTI3.08 TTI5.03
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	TTI1.01 TTI1.05 TTI3.01 TTI3.02 TTI3.03 TTI3.08 TTI5.01 TTI5.02 TTI5.03

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Logical and Physical Access Controls		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	TTI6.01 TTI6.02 TTI6.03
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	TTI3.04 TTI6.02
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	TTI3.04 TTI6.02 TTI6.04
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	TTI6.05
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	TTI6.05
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	TTI2.01 TTI6.06
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	TTI6.01 TTI6.03
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	TTI4.01

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

System Operations		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	TTI3.02 TTI3.06
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	TTI2.01 TTI4.01 TTI6.01
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	TTI7.01
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	TTI1.14 TTI7.01
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	TTI1.14 TTI5.01 TTI7.01 TTI7.02

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Change Management		
Trust Services Criteria	Trust Services Criteria Description	Controls Provided by TeachTown, Inc. (TTI)
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	TTI3.06 TTI3.08 TTI3.09
Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	TTI3.01 TTI3.02 TTI3.06 TTI7.02 TTI8.01
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	TTI3.03 TTI3.07 TTI8.02

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.01	Policies and procedures are formally documented to ensure that internal controls are met. They are updated as needed, but reviewed and approved at least annually.	CC1.1 CC2.2 CC5.1 CC5.2 CC5.3	Inspected TeachTown's policies and procedures and validated that they define the Company's internal controls of which are outlined in this report. Validated that they include a last review and approval date within the audit period, or past year.	No exceptions noted.
TTI1.02	On a monthly basis, Company-wide meetings are held. Key personnel presenting in these meetings discuss the state of the Company, key initiatives, and TeachTown's core values.	CC1.1 CC2.2	For a random, representative sample of months within the audit period, inspected evidence and validated that a Company-wide meeting was held. Inspected further evidence and validated that key personnel presented and discussed the state of the Company, key initiatives, and TeachTown's core values during the meeting.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.03 Contractors are used by the Company when needed. Contractor workers are required to sign a contractor agreement prior to being employed by TeachTown.	CC1.1 CC1.4 CC1.5 CC2.3	For a random, representative sample of new contractors within the audit period, inspected evidence and validated that a contractor agreement is in place between TeachTown and the contractor and has been signed by both parties.	No exceptions noted.
TTI1.04 Vendor agreements must be in place before a third-party provides services to TeachTown. If the vendor has access to confidential information, such contracts should include appropriate disclosures surrounding privacy, confidentiality, and unauthorized access and reporting.	CC1.1 CC2.3	For a random, representative sample of new third-party vendors within the audit period, inspected evidence and validated that a vendor agreement is in place between TeachTown and the vendor and has been signed by both parties. As applicable, validated that the agreement includes disclosures surrounding privacy, confidentiality, and unauthorized access and reporting.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TT11.05	An Employment Handbook and Acceptable Use Policy (AUP) are in place that outline the Company's expectations that employees are to be informed on and follow. At hire, employees are required to sign an acknowledgement form stating they have read, understand and agree to the handbook and AUP.	CC1.1 CC1.4 CC1.5 CC2.2 CC5.3	Inspected TeachTown's Employment Handbook and AUP and validated that they outline the Company's expectations of employees.	No exceptions noted.
			For a random, representative sample of new employees within the audit period, inspected evidence and validated that the individual signed the handbook and AUP acknowledgement form at hire.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TT11.06 A Board of Directors is in place that meets on a quarterly basis. An agenda and meeting minutes are documented and maintained. The roles and responsibilities of Board members are documented, which state that the majority of Board members must be independent from management. Upon joining the Board, members are required to sign a Board agreement stating they have read, understand and agree to their roles and responsibilities. The agreement covers conflict of interest statements.	CC1.2 CC1.5 CC2.2	For a random, representative sample of quarters within the audit period, inspected evidence and validated that a Board of Directors meeting was held. Inspected further evidence and validated that an agenda and meeting minutes were documented. Inspected evidence and validated that the roles and responsibilities of Board members are documented, which state that the majority of Board members must be independent from management. For the total population of Board members, inspected evidence and validated that the majority are independent from management. For a random, representative sample of new Board members within the audit period, inspected evidence and validated that a Board agreement was signed during onboarding. Validated that the agreement covers conflict of interest statements.	No exceptions noted. No exceptions noted. No exceptions noted. No instances occurred, and therefore, the operational effectiveness of this control was not determined.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.07 An Executive Leadership Team is in place that meets on a weekly basis to ensure Company goals and objectives are being met and monitored. An agenda and meeting minutes are documented and maintained.	CC1.3 CC2.2	For a random, representative sample of weeks within the audit period, inspected evidence and validated that an Executive Leadership Team meeting was held. Inspected further evidence and validated that an agenda and meeting minutes were documented.	No exceptions noted.
TTI1.08 A Product Leadership Team is in place that meets on a weekly basis to ensure the Company's information technology (IT), engineering and product objectives and timelines are being met and monitored. An agenda and meeting minutes are documented and maintained.	CC1.3 CC2.2	For a random, representative sample of weeks within the audit period, inspected evidence and validated that a Product Leadership Team meeting was held. Inspected further evidence and validated that an agenda and meeting minutes were documented.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.09	An Information Security and Privacy Team is in place that meets on a weekly basis to ensure the Company remains in compliant with its security and privacy requirements. An agenda and meeting minutes are documented and maintained.	CC1.3 CC2.2	For a random, representative sample of weeks within the audit period, inspected evidence and validated that an Information Security and Privacy Team meeting was held. Inspected further evidence and validated that an agenda and meeting minutes were documented.	No exceptions noted.
TTI1.10	A Security Operations Center Team is in place that meets on a bi-weekly basis to ensure the Company's operations are being met and monitored, and that operational updates are discussed. An agenda and meeting minutes are documented and maintained.	CC1.3 CC2.2	For a random, representative sample of months within the audit period, inspected evidence and validated that, at least two, Security Operations Center Team meetings were held. Inspected further evidence and validated that an agenda and meeting minutes were documented.	No instances occurred, and therefore, the operational effectiveness of this control was not determined.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.11	An organizational chart is in place to ensure that the current roles and relationships between individuals within the Company have been established. The chart is updated as needed based on employment changes.	CC1.3	Inspected evidence and validated that an up-to-date organizational chart is in place.	No exceptions noted.
TTI1.12	Job descriptions are established for candidates for employment that define the open position's qualification, roles, and responsibilities requirements.	CC1.3 CC1.5 CC2.2	For a random, representative sample of new employees within the audit period, inspected evidence and validated that the individual has a documented job description in place. Validated that the description defines the position's qualifications, roles, and responsibilities requirements.	For 1 out of the 4 new hires sampled, a job description is not in place.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.13	A formal hiring process is in place to ensure candidates for employment are sufficiently interviewed and vetted. Background and reference checks are required prior to hiring. Once hired, employees are required to go through new hire training.	CC1.4	For a random, representative sample of new employees within the audit period, inspected evidence and validated that an interview and vetting process took place for the new hire prior to onboarding. For a random, representative sample of new employees within the audit period, inspected evidence and validated that reference checks were completed prior to hiring. For a random, representative sample of new employees within the audit period, inspected evidence and validated that background checks were completed prior to hiring. For a random, representative sample of new employees within the audit period, inspected evidence and validated that the individual completed new hire training at hire.	No exceptions noted. For 4 out of the 4 new hires sampled, reference checks were not completed. For 1 out of the 4 new hires sampled, a background check was not completed before hire. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI1.14	Employees and contractors with access to internal information must complete security and privacy training at hire and on an annual basis thereafter. The training covers the Company's policies and procedures, including how employees are to identify and report on security incidents.	CC1.4 CC2.2 CC7.4 CC7.5	For a random, representative sample of new employees within the audit period, inspected evidence and validated that the individual completed security and privacy training at hire, as applicable. For a random, representative sample of new contractors within the audit period, inspected evidence and validated that the individual completed security and privacy training at hire, as applicable. For a random, representative sample of current employees that have been employed by the Company for at least 12 months, inspected evidence and validated that the individual completed security and privacy training within the audit period, or past year, as applicable. For a random, representative sample of current contractors that have been employed by the Company for at least 12 months, inspected evidence and validated that the individual completed security and privacy training within the audit period, or past year, as applicable.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
TTI1.15	On an annual basis, employee performance reviews take place. Such reviews are documented and maintained.	CC1.4 CC1.5	For a random, representative sample of current employees that have been employed by the Company for at least 12 months, inspected evidence and validated that the individual had a performance review completed within the audit period, or past year.	For 13 out of the 13 current employees sampled, performance reviews did not take place within the audit period, or past year.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TT11.16	Procedures are in place to ensure employee and contractor misconducts are handled and documented.	CC1.5	Inspected TeachTown's policies and procedures and validated that employee and contractor misconduct handling processes are in place. For a random, representative sample of employee and contractor misconducts from within the audit period, inspected evidence and validated that the issues were handled and documented as required.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI2.01	A security information and event management (SIEM) tool is in place that is provided and monitored by an independent third-party. When required, TeachTown will work with third-party personnel to address and remediate any issues identified by the tool. In addition, the Company's environment is hosted by another independent third-party, Amazon Web Services (AWS). Service offerings by AWS have been subscribed to in order to monitor the environment's stateless and web application firewalls. Relevant security logs have been synced to the SIEM tool.	CC2.1 CC2.3 CC6.6 CC7.2 Inspected evidence and validated that a SIEM tool is in place. Inspected evidence and validated that the SIEM tool has been configured to monitor and report on TeachTown's in-scope environment. Inspected evidence and validated that users have been configured to be alerted of SIEM events categorized as an incident. Inspected evidence and validated that TeachTown is subscribed to service offerings provided by AWS to monitor its environment's stateless and web application firewalls. Inspected evidence and validated that AWS security logs have been configured to be synced with the SIEM tool.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI2.02	Email, Slack and Salesforce are utilized as the Company's main platforms for internal and external communication.	CC2.2 CC2.3	Inspected evidence and validated that email, Slack and Salesforce are utilized as the Company's main platforms for internal and external communication.	No exceptions noted.
TTI2.03	Contact and service information is available on the Company's website for external parties.	CC2.3	Inspected TeachTown's website and validated that contact and service information is available to external parties.	No exceptions noted.
TTI2.04	A Terms of Service and Privacy Notice are available on the Company's website. The Privacy Notice is clearly dated and describes how TeachTown collects, uses and discloses of personal information.	CC2.3	Inspected TeachTown's website and validated that the Company's Terms of Service and Privacy Notice are available to external parties. Inspected TeachTown's Privacy Notice and validated that it is clearly dated and describes how the Company collects, uses and discloses of personal information.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI2.05 When a user signs up for an account via TeachTown's website, as a part of the sign up process, they are required to acknowledge that they have read and agree to the End User License Agreement and the Facilitator Agreement. Within the Facilitator Agreement, a reference to the Company's Privacy Notice is included. Once an account has been successfully created, the user can access and modify their information as desired.	CC2.3	Inspected evidence and validated that, when a user signs up for an account via TeachTown's website, as a part of the sign up process, they are required to acknowledge that they have read and agree to the End User License Agreement and the Facilitator Agreement. Inspected evidence and validated that, once an account has been successfully created, a user can access and modify their information as desired.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.01	A Risk Management Policy is in place that outlines how the Company is to identify, assess, monitor, remediate, and report on newly identified and existing risks.	CC3.1 CC5.1 CC5.3 CC9.1	Inspected evidence and validated that a Risk Management Policy is in place that outlines how the Company is to identify, assess, monitor, remediate, and report on newly identified and existing risks.	No exceptions noted.
TTI3.02	A Vulnerability and Patch Management Policy is in place that outlines how the Company is to identify, evaluate, treat, and report on security vulnerabilities in systems and the software that runs on them.	CC3.1 CC5.1 CC5.2 CC5.3 CC7.1 CC9.1	Inspected evidence and validated that a Vulnerability and Patch Management Policy is in place that outlines how the Company is to identify, evaluate, treat, and report on security vulnerabilities in systems and the software that runs on them.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.03	A Vendor Management Policy is in place that outlines how the Company is to select and manage external third-parties that the Company utilizes for support.	CC3.1 CC5.1 CC5.3 CC9.2	Inspected evidence and validated that a Vendor Management Policy is in place that outlines how the Company is to select and manage external third-parties that the Company utilizes for support.	No exceptions noted.
TTI3.04	Security role user groups are in place to ensure that user access is granted on an as needed basis based on job roles and responsibilities for internal users. Privileged and elevated access is limited.	CC3.1 CC3.3 CC6.2 CC6.3	Inspected evidence and validated that security role user groups are in place. Inspected evidence and validated that user roles tied to employee user accounts have been granted on a need-to-have (restricted) basis, and that privileged and elevated access has been limited as defined by TeachTown.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.05	On an annual basis, an independent third-party is contracted to perform a risk assessment of the Company's environment. The results are reviewed and corrective action plans are documented in a risk register. The potential for fraud is included as a part of the assessment performed.	CC3.2 CC3.3	Inspected evidence and validated that an independent third-party risk assessment was conducted within the audit period, or past year. Validated that the potential for fraud was included as a part of the assessment.	No exceptions noted.
			Inspected evidence and validated that the results from the most recent independent third-party risk assessment conducted have been formally reviewed by TeachTown personnel. Validated that corrective action plans have been documented within a risk register.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.06	External and credentialed vulnerability scans are conducted on a weekly basis using AWS provided vulnerability scanning technologies. Vulnerabilities are reviewed and remediated, as required. Remediation efforts are documented and maintained.	CC3.2 CC4.1 CC7.1 CC8.1 CC9.1	For a random, representative sample of weeks within the audit period, inspected evidence and validated that external and credentialed vulnerability scans were completed. Validated that the vulnerabilities identified from the scans were formally reviewed. Validated that remediation plans were completed (as deemed necessary) and documented.	No exceptions noted.
TTI3.07	On an annual basis, the Company requests and formally reviews assurance documentation from the applicable subservice organizations in-scope.	CC3.2 CC4.1 CC4.2 CC9.2	For the total population of subservice organizations in-scope, inspected evidence and validated that TeachTown personnel have collected most recent copies of the vendors' SOC 2 Type 2 reports. Validated that there is documentation to show that the reports have been formally reviewed and that assurance has been received by the Company based on the review.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.08	A Change Management Policy is in place that defines the different levels of changes and the requirements that must be followed based on each type or risk.	CC3.4 CC5.2 CC5.3 CC8.1	Inspected evidence and validated that a Change Management Policy is in place that defines the different levels of changes and the requirements that must be followed based on each type or risk.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI3.09 Technical changes are tracked within the Company's ticketing system and the ticket must show that a formal review, approval, and testing has been completed prior to the change being implemented. The changes must show through documentation that the segregation of duties was present. In addition, changes that are deemed major or significant by TeachTown require a backout plan to be established and agreed upon by all stakeholders and project team members.	CC3.4 CC8.1	For a random, representative sample of everyday/standard technical changes within the audit period, inspected evidence and validated that the changes were formally documented showing they were requested, reviewed, approved, tested, and that proper segregation of duties was present prior to the changes being implemented. For a random, representative sample of major/significant technical changes within the audit period, inspected evidence and validated that the changes were formally documented showing they were requested, reviewed, approved, tested, and that proper segregation of duties was present prior to the changes being implemented. Inspected further evidence and validated that a backout plan was established and agreed upon by all stakeholders and project team members.	Evidence was not retained by the Company in order to test the operational effectiveness of everyday/standard technical changes from within the audit period. For 60 out of the 60 major/significant technical changes sampled, a backout plan was not established and agreed upon by all stakeholders and project team members.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI4.01	Endpoint protection is implemented and maintained on all laptops and workstations. Automatic updates are configured and real-time scanning is enabled. Administrative access to the solution is restricted to appropriate personnel as defined by TeachTown.	CC4.1 CC6.8 CC7.2	Inspected evidence and validated that endpoint protection is implemented and maintained on all laptops and workstations. Inspected evidence and validated that the endpoint protection provides automatic updates. Inspected evidence and validated that the endpoint protection provides real-time scanning. Inspected evidence and validated that administrative access to the endpoint protection console is restricted as defined by TeachTown.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI5.01 An Incident Response Plan is in place which outlines steps on how to detect, report, respond to, and recover from security incidents and breaches. The Company's Incident Response Plan is tested on an annual basis.	CC5.1 CC5.3 CC7.5	Inspected evidence and validated that an Incident Response Plan is in place which outlines steps on how to detect, report, respond to, and recover from security incidents and breaches. Inspected evidence and validated that the Company's Incident Response Plan was tested within the audit period, or past year. For a random, representative sample of technical incidents and breaches from within the audit period, inspected evidence and validated that the incidents were handled as required and resolution documentation is in place. For a random, representative sample of privacy violation incidents from within the audit period, inspected evidence and validated that the incidents were handled as required and resolution documentation is in place.	No exceptions noted. No exceptions noted. No instances occurred, and therefore, the operational effectiveness of this control was not determined. No instances occurred, and therefore, the operational effectiveness of this control was not determined.
TTI5.02 An Information Protection Policy is in place which outlines the classifications of the types of data in which the Company collects, and depending on that classification, how such data is to be handled.	CC5.1 CC5.3	Inspected evidence and validated that an Information Protection Policy is in place which outlines the classifications of the types of data in which the Company collects, and depending on that classification, how such data is to be handled.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI5.03 A Data Retention, Destruction, and Transfer Policy is in place which outlines how the Company is to securely maintain, handle and dispose of data and destruct old hardware. <i>Note: Such responsibilities have been carved out to AWS at this time.</i>	CC5.1 CC5.2 CC5.3	Inspected evidence and validated that a Data Retention, Destruction, and Transfer Policy is in place which outlines how the Company is to securely maintain, handle and dispose of data and destruct old hardware. Inspected evidence and validated that TeachTown personnel have collected most recent copies of AWS' SOC 2 Type 2 reports. Validated that there is documentation to show that the reports have been formally reviewed and that assurance has been received by the Company based on the review.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI6.01	The laptops and workstations in use are provided by the Company and a mobile device management tool is in place to inventory, monitor and manage such devices. The tool allows TeachTown to remotely wipe a device if it were to be reported lost or stolen.	CC6.1 CC6.7 CC7.2	Inspected evidence and validated that a mobile device management tool is in place and implemented and maintained on all laptops and workstations. Inspected evidence and validated that the mobile device management tool has remote wipe capabilities.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI6.02 Remote access to the AWS environment requires a virtual private network (VPN) connection. A unique user ID, password, and second-factor authentication is enforced. Minimum password and lockout settings are configured and enforced. In addition, user access modifications are handled by an independent third-party after requests are submitted via a ticketing system by TeachTown personnel. When an employee is terminated, access is required to be revoked at the booked time, or immediately for unplanned terminations.	CC6.1 CC6.2 CC6.3	Inspected evidence and validated that remote access to the AWS environment requires a VPN connection. Inspected evidence and validated that an unique user ID, password, and second-factor authentication is enforced for VPN connections. Inspected evidence and validated that minimum password and lockout settings are configured and enforced for VPN connections. For a random, representative sample of new employees within the audit period, inspected evidence and validated that an authorized user access request was submitted via a ticketing system by TeachTown personnel. For a random, representative sample of new contractors within the audit period, inspected evidence and validated that an authorized user access request was submitted via a ticketing system by TeachTown personnel. For a random, representative sample of employee position changes requiring modified access within the audit period, inspected evidence and validated that an authorized user access modification request was submitted via a ticketing system by TeachTown personnel. For a random, representative sample of contractor position changes requiring modified access within the audit period, inspected evidence and validated that an authorized user access modification request was submitted via a ticketing system by TeachTown personnel.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted. No instances occurred, and therefore, the operational effectiveness of this control was not determined. No instances occurred, and therefore, the operational effectiveness of this control was not determined.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI6.02 (Cont.)			For a random, representative sample of employees terminated within the audit period, inspected evidence and validated that an authorized user access removal request was submitted via a ticketing system by TeachTown personnel. For a random, representative sample of contractors terminated within the audit period, inspected evidence and validated that an authorized user access removal request was submitted via a ticketing system by TeachTown personnel.	No exceptions noted. A process is not currently in place for tracking when a contractor is terminated, and therefore, Bonadio was unable to sufficiently test the operational effectiveness of this control.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI6.03	All laptop and workstation hard drives are encrypted.	CC6.1 CC6.7	For a random, representative sample of current employees within the audit period, inspected evidence and validated that the individual's laptop and/or workstation hard drive(s) is/are encrypted. For a random, representative sample of current contractors within the audit period, inspected evidence and validated that the individual's laptop and/or workstation hard drive(s) is/are encrypted.	No exceptions noted. For 5 out of the 5 current contractors sampled, the individuals' laptop and/or workstation hard drives are not encrypted.
TTI6.04	User access reviews are performed and documented on a quarterly basis to ensure that all authorized access roles remain appropriate.	CC6.3	For a random, representative sample of quarters within the audit period, inspected evidence and validated that a user access review was performed and documented.	No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI6.05	On an annual basis, the Company requests and formally reviews assurance documentation from AWS to ensure suitably designed and operating controls around CC6.4 and CC6.5 are in place and reported on.	CC6.4 CC6.5	Inspected evidence and validated that TeachTown personnel have collected most recent copies of AWS' SOC 2 Type 2 reports. Validated that there is documentation to show that the reports have been formally reviewed and that assurance has been received by the Company based on the review.	No exceptions noted.
TTI6.06	Access to the configuration of the AWS firewalls is restricted to appropriate personnel as defined by TeachTown. Firewall rules have been implemented to appropriately restrict network traffic.	CC6.6	Inspected evidence and validated that administrative access to the configuration of the AWS firewalls is restricted to appropriate personnel as defined by TeachTown. Inspected evidence and validated that firewall rules have been implemented to appropriately restrict network traffic.	No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI7.01 The review, and if required remediation, of technical incidents and breaches are handled and documented by a third party with support from TeachTown personnel as required. The handling of organizational potential incidents and breaches follow the Company's Incident Response Plan. This process also covers the handling of privacy violations, responses, and resolution of any unauthorized disclosures.	CC7.3 CC7.4 CC7.5	Inspected evidence and validated that an Incident Response Plan is in place which outlines the Company's handling steps of organizational potential incidents and breaches, as well as privacy violations, responses, and resolution of any unauthorized disclosures. For a random, representative sample of technical incidents and breaches from within the audit period, inspected evidence and validated that the incidents were handled as required and resolution documentation is in place. For a random, representative sample of privacy violation incidents from within the audit period, inspected evidence and validated that the incidents were handled as required and resolution documentation is in place.	No exceptions noted. No instances occurred, and therefore, the operational effectiveness of this control was not determined. No instances occurred, and therefore, the operational effectiveness of this control was not determined.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.	Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI7.02 Backups of data are performed by AWS on a daily basis and backup failure alerting has been configured. Per AWS' SOC 2 Type 2 Report, backups are encrypted. Administrative access to the backup information and settings are restricted to appropriate personnel as defined by TeachTown.	CC7.5 CC9.1	Inspected evidence and validated that TeachTown personnel have collected most recent copies of AWS' SOC 2 Type 2 reports. Validated that there is documentation to show that the reports have been formally reviewed and that assurance has been received by the Company based on the review. Inspected evidence and validated that backups of data stored within AWS are scheduled to be performed automatically on a daily basis. Inspected evidence and validated that backup failure alerting has been configured. Inspected evidence and validated that administrative access to the backup information and settings are restricted to appropriate personnel as defined by TeachTown.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS (CONTINUED)

Controls Provided by TeachTown, Inc.		Related Trust Services Criteria	Tests Performed by Bonadio & Co., LLP	Results Provided by Bonadio & Co., LLP
TTI8.01	Cyber liability insurance is in place and maintained.	CC9.1	Inspected evidence and validated that cyber liability insurance is in place that covered the period under audit.	No exceptions noted.
TTI8.02	Vendor due diligence procedures are formally documented to ensure that the Company has appropriately evaluated the vendor's control objectives and commitments prior to contracting.	CC9.2	For a random, representative sample of new third-party vendors from within the audit period, inspected evidence and validated that vendor due diligence was performed prior to contracting.	No exceptions noted.

SECTION FIVE

**Other Information Provided by TeachTown, Inc. That is Not Covered by
the Service Auditor's Report**

OTHER INFORMATION PROVIDED BY TEACHTOWN, INC. THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT

Management's Response to Control Exceptions

The table below contains Management's response to the exceptions identified in Section 4 above.

Control Activity	Management Response
TTI1.12: Job descriptions are established for candidates for employment that define the open position's qualification, roles, and responsibilities requirements. Exception Noted: For 1 out of the 4 new hires sampled, a job description is not in place.	The noted exception was related to a unique situation. TeachTown had an employee working in a part-time role who had expressed interest a full-time position. TeachTown determined that this employee was a strong candidate for that role, but there was not a vacancy at that time. When a full-time employee departed the Company, that departure opened up the role the part-time employee was interested in. Rather than post the vacancy externally, TeachTown opted to offer the full-time role to that part-time employee. Going forward, TeachTown plans to draft job descriptions for open roles where a job description does not currently exist.
TTI1.13: A formal hiring process is in place to ensure candidates for employment are sufficiently interviewed and vetted. Background and reference checks are required prior to hiring. Once hired, employees are required to go through new hire training. Exceptions Noted: For 4 out of the 4 new hires sampled, reference checks were not completed. For 1 out of the 4 new hires sampled, a background check was not completed before hire.	The one noted exception regarding a gap in a background check was for an individual that was onboarded to support TeachTown in a part-time capacity prior to being hired as a full-time employee in September 2023. The background check in question was completed in June 2023 prior to TeachTown extending an offer for full-time employment. Going forward, TeachTown will ensure background checks are conducted for part-time hires as well. Additionally, TeachTown has updated its recruitment process in September 2023 to include reference checks for new hires. This updated process is currently in effect.
TTI1.15: On an annual basis, employee performance reviews take place. Such reviews are documented and maintained. Exceptions Noted: For 13 out of the 13 current employees sampled, performance reviews did not take place within the audit period, or past year.	TeachTown hired a HR Director in 2022 and she is implementing a tracking procedure for performing performance reviews. TeachTown plans to implement that tracking procedure in quarter 1 of 2024.

OTHER INFORMATION PROVIDED BY TEACHTOWN, INC. THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT (CONTINUED)

Management's Response to Control Exceptions (Continued)

Control Activity	Management Response
TTI3.09: Technical changes are tracked within the Company's ticketing system and the ticket must show a formal review, approval, and testing has been completed prior to the change being implemented. The changes must show through documentation that the segregation of duties was present. In addition, changes that are deemed major or significant by TeachTown require a backout plan to be established and agreed upon by all stakeholders and project team members. Exceptions Noted: Evidence was not retained by the Company in order to test the operational effectiveness of everyday/standard technical changes from within the audit period. For 60 out of the 60 major/significant technical changes sampled, a backout plan was not established and agreed upon by all stakeholders and project team members.	On October 24, 2023, TeachTown updated the CloudWatch log group in AWS to include an extended duration of logs. The current configuration now meets the retention period associated with this control. Additionally, TeachTown will update its change control processes and procedures to ensure that backout plans are established and agreed upon by all stakeholders and project team members when major and significant changes occur.
TTI6.02: Remote access to the AWS environment requires a virtual private network (VPN) connection. A unique user ID, password, and second-factor authentication is enforced. Minimum password and lockout settings are configured and enforced. In addition, user access modifications are handled by an independent third-party after requests are submitted via a ticketing system by TeachTown personnel. When an employee is terminated, access is required to be revoked at the booked time, or immediately for unplanned terminations. Exception Noted: A process is not currently in place for tracking when a contractor is terminated, and therefore, Bonadio was unable to sufficiently test the operational effectiveness of this control.	TeachTown hired a HR Director in 2022 and she is implementing a tracking procedure for tracking terminated contractors. TeachTown plans to implement that tracking procedure in quarter 1 of 2024. At present, TeachTown considers this to be a low risk exception as no contractors have access to student data.

OTHER INFORMATION PROVIDED BY TEACHTOWN, INC. THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT (CONTINUED)

Management's Response to Control Exceptions (Continued)

Control Activity	Management Response
TTI6.03: All laptop and workstation hard drives are encrypted. Exceptions Noted: For 5 out of the 5 current contractors sampled, the individuals' laptop and/or workstation hard drives are not encrypted.	The majority of TeachTown contractors do not have access to data that requires encryption (as defined in TeachTown's Information Protection Policy). In the event that a contractor's duties may require access to sensitive systems or data, that contractor is provided a fully-managed laptop by TeachTown's IT department. These laptops are all encrypted, as demonstrated in evidence provided by TeachTown's managed services provider. TeachTown plans to address this exception to update the language in the Information Security Policy to more accurately reflect how the Company is managing this risk and the supporting controls.



TEACHTOWN®

Exceptional Solutions for Exceptional Students

Technical and Security Overview

Version January 2026



PURPOSE

This document is intended to provide you with an overview of TeachTown and our technology and security protocols that are used within the TeachTown products and platform. For security reasons some detail has been omitted to protect the integrity of our products.

COMPANY OVERVIEW

- **Name/Company Name:** Jigsaw Learning LLC, dba TechTown
- **Company Website:** www.teachtown.com
- **Company Address and Phone:** 2 Constitution Way Woburn MA 01801. 1-800-283-0165
- **Privacy Policy:** web.teachtown.com/privacy-policy/
- **Terms of Service:** web.teachtown.com/terms-of-service/
- **Technical Support:** support@teachtown.com

SYSTEM REQUIREMENTS AND SERVER INFRASTRUCTURE

TeachTown software products are “Software as a Service” (SaaS) applications hosted by AWS in the United States and are available 24/7. A supported web browser and an Internet connection are required to access TeachTown products. TeachTown staff will perform the initial provisioning based on your programs including your staff logins (administrators, teachers, etc...). Account activation occurs at the start of the TeachTown subscription date.

In addition to the basic configurations, SSO (SAML) can be set up. We also have integrations with OneRoster, Clever and ClassLink.

These are our system requirements:

Browser-based applications:

- High speed internet connection – DSL or Cable (1 Mbps) recommended
- Any modern HTML5-compliant browser
- Minimum screen resolution 1024×768
- Runs on any computer or device that will run a supported browser noted above

iPad applications via Apps:

- Installed via Apple App Store.
- iOS v18 or greater
- Apps should work on all iPad models that support iOS 18.
- High speed internet connection – DSL or Cable (1 Mbps) recommended. However, most applications are capable of running off line or on slower internet connections once content has been cached locally

Chromebook:

- Apps must be run in the Chrome browser at teachtown.com
- High speed internet connection – DSL or Cable (1 Mbps) recommended
- Minimum screen resolution 1024×768
- Supports touch screen if present

DATA CENTER SECURITY & INFORMATION LIFECYCLE MANAGEMENT

Data Center and Data Location

Your data will be hosted in **Amazon Web Services (AWS)** within their data centers located in the **United States**. AWS does not permit non-employees access to their data center facilities. Logical access is restricted using industry best practices for hosting applications with Public Cloud Service providers. AWS Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provide additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television cameras (CCTV) as defined in the AWS Data Center Physical Security Policy."

Data Encryption

As tenants of Amazon Web Services, we naturally adopt the usage of Amazon's proprietary overlay protocol utilized when systems in our environment need to communicate with each other via public networks. Data sent over public networks is encrypted using an implementation recommended by the National Institute of Standards and Technology (NIST). Similarly, NIST leading practices for encrypting data at rest and in motion are implemented. Data is encrypted at rest and in motion

Data Access

Access to your school or district's data requires a valid user account, username, and password. An authorized user with the appropriate user permissions can create user accounts. All users are required to initiate a valid session, which expires after 60 minutes of inactivity. All sign-ins by users authorized to view school data are logged with a timestamp, account ID, and IP address. Any pages that require a user to enter their account information are encrypted using SSL. All passwords are stored in the database in an encrypted format created with a one-way hash.

Data Backups

Client data is backed up nightly both locally and remotely.

APPLICATION & INTERFACE SECURITY

Vulnerability Scanning

TeachTown utilizes an enterprise grade vulnerability scanning capability to scan our systems on a regular cadence and update systems in accordance with internally established standards..

Data Integrity

We have implemented several mechanisms to verify data integrity including but not limited to the following: logic to maintain data synchronization between data stores, implementation of transport layer security (TLS) with the appropriate cipher suites enabling for integrity. Additionally, we regularly test data integrity via automated restoration of data to our reporting environment.

BUSINESS CONTINUITY & OPERATIONAL RESILIENCE

BCDR

Our Business Continuity Policies and Plans have been developed in alignment with Control Objectives for Information and Related Technologies (COBIT) guidance. We have planned tests on our systems.

Retention Policy

We backup data in alignment with contractual, and applicable regulatory and statutory requirements. We test our database backups nightly by performing full restorations to our reporting environments.

DATA SECURITY & INFORMATION LIFECYCLE MANAGEMENT

eCommerce Transactions

TeachTown uses industry standard TLS 1.2 AES-256 for all client-server interactions. As tenants of Amazon Web Services, we naturally adopt the usage of Amazon's proprietary overlay protocol utilized when systems in our environment need to communicate with each other via public networks. Data sent over these networks is encrypted.

Non Production Data

We utilize virtual desktop interfaces to securely access data in our environments. As such, no data leaves our cloud environment. Additionally, our non-production environment utilizes the same controls as noted above.

Secure Disposal

We have a documented procedure outlining the steps taken to sanitize all computing resources of tenant personally identifiable information when provided with a request from an individual or entity to do so. As tenants of Amazon Web Services, we rely upon the industry recognized techniques (NIST 800-88) for decommissioning storage nodes that provide a level of assurance that customer data is not exposed to unauthorized individuals.

Asset Management

In alignment with NIST Cybersecurity Framework (CSF), TeachTown assets are assigned owners and are tracked and monitored.

SOC2 Type 2 Certification

TeachTown is SOC II TYPE II certified and operates its controls to provide assurance of ongoing SOC II Type II obligations.

Data Privacy

Privacy Oversight and Laws

TeachTown maintains a comprehensive privacy program to address the data we collect, use and disclose as a result of the operation of our online solution. We consider personal information, including student data, to be confidential and do not use student data for any purpose other than to provide the service on our client's behalf, in accordance with any contractual agreements with our clients. Our collection, use disclosure of student data is in accordance with our Terms of Service and/or any other agreement with a client, and by the provisions of the Family Educational Rights and Privacy Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Children's Online Privacy Protection Act ("COPPA"), and applicable state laws which relate to the collection, use and disclosure of student data. We collect, maintain, use and share student data only for an authorized educational purpose and as described in our agreement with our client, or as directed by our clients. For more information on how we collect, process, store and share data, please refer to our published [privacy notice](#).

Data Policies

We have a documented Data Privacy Notice on our website as noted above. In addition, Teachtown has a documented internal Global Privacy Policy.

Training/Awareness

We provide privacy training and awareness to all employees annually with refreshers throughout the year. Training is also conducted upon hire.

Controls & Reporting

TeachTown further has reporting controls in place to allow employees, contractors, service providers or clients to report unauthorized use or disclosure of data, as well as concerns with how TeachTown administers its privacy responsibilities.

GOVERNANCE & RISK MANAGEMENT

Baseline Requirements

We utilize established baseline secure configuration standards for infrastructure that is our responsibility as per the shared responsibility model.

Policy, Policy Enforcement & Review

TeachTown implements formal, documented policies and procedures that provide guidance for operations and information security within the organization. The policies address purpose, scope, ownership, roles and responsibilities. Employees who violate TeachTown standards and/or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. TeachTown information security and/or privacy policies are reviewed and approved on an annual basis at a minimum by leadership.

HUMAN RESOURCES

Asset Returns and Termination

Upon termination, we execute our offboarding procedures, which include steps for access removal and collection of assets.

Background Screening & Employee Agreements

We conduct criminal background checks, as permitted by applicable law, for employees who perform onsite training and coaching and/or are in the classroom interacting with teachers or students, as well as employees who have access to student data.

Training/Awareness

We provide cybersecurity and privacy training and awareness to all employees annually with refreshers throughout the year. Training is also conducted upon hire. Our cybersecurity training and awareness program is built in alignment with the NIST CSF framework and incorporates privacy rules and regulations.

IDENTITY & ACCESS MANAGEMENT

Audit Tool Access

We restrict, log, and monitor access to our information security systems. We utilize a Managed Security Service Provider (MSSP) Security Operations Center (SOC) to monitor logs from these systems. Additionally, we conduct periodic access reviews and take the appropriate action to revoke or reduce privileges, where necessary. We have identified auditable event/log categories across systems in our environment. As such, the system owners have configured these systems to record continuously the security-related events in accordance with requirements. These logs are monitored by our Managed Security Service Provider (MSSP) Security Operations Center (SOC) and anomalous activity is alerted appropriately for review and analysis.

User Access Policy & Procedures

As per our offboarding standard operating procedure, access that is no longer required is

revoked accordingly. Periodically, we audit this standard operating procedure to assess the procedures operating effectiveness. We utilize a centralized directory service and an identity and access management (IAM) capability to manage and store the identity of all personnel who have access to the IT infrastructure.

Source Code Access & Restriction

We utilize logical access controls to prevent unauthorized access to the application and/or source code. Examples of these logical access controls include: a Web Application Firewall (WAF) and AWS Identity and Access Management (IAM) policies configured in alignment with least privilege principles. We utilize role based access controls (RBAC) to prevent unauthorized access.

User Access

We utilize our change management procedures as the mechanism to document and approve access requests. Approved granted access is governed by logical access control policies configured in alignment with least privilege principles through the usage of AWS Identity and Access Management (IAM). We conduct periodic access reviews for administrators who have access to sensitive data. If excess privileges are found, they are revoked. As per our offboarding standard operating procedure, access that is no longer required is revoked accordingly. Periodically, we audit this standard operating procedure to assess the procedures operating effectiveness.

INFRASTRUCTURE & VIRTUALIZATION SECURITY

Audit Logging & Intrusion Detection

We utilize an enterprise grade anti-malware/anti-virus, endpoint detection, and response (EDR) capability for systems in our environment. This capability naturally provides detections needed to respond to possible incidents. In accordance with least privilege principles, access to audit logs are restricted to authorized personnel. We have identified auditable event/log categories across systems in our environment. As such, the system owners have configured these systems to record continuously the security-related events in accordance with requirements. These logs are monitored by our Managed Security Service Provider (MSSP) Security Operations Center (SOC) and anomalous activity is alerted appropriately for review and analysis.

OS Hardening & Base Controls

We utilize several mandatory technical controls for workstations in our environment. Some examples include: host based firewall with strict port/protocols limitations, anti-virus/anti-malware, endpoint detection and response (EDR), and patch management. Similarly, we utilize the same mandatory technical controls within our server environment, with some notable additions including: hardened images in alignment with industry recognized authoritative sources on configuration management, network based firewall, and vulnerability

scanning. We utilize a Web Application Firewall (WAF) and network based firewall to protect systems from unauthorized access.

AWS Security

As tenants of Amazon Web Services, we rely on our cloud providers' controls in regards to privilege access for administrative consoles. AWS states the following: "AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls"

Wireless Security

As tenants of Amazon Web Services, we rely on our cloud providers' controls in regards to the protection of the AWS wireless network environment. AWS states the following: "There are no wireless networks or radio signals within the system boundary. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system. AWS continuously monitors wireless networks in order to detect rogue or other devices not authorized to authenticate to the system."

SECURITY INCIDENT MANAGEMENT, E-DISCOVERY & CLOUD FORENSICS

Incident Management

Our incident response plan has been developed in alignment with several incident response related control objectives articulated in the NIST CSF framework alongside NIST Special Publication (SP) 800-61 (Computer Security Incident Handling Guide).

Incident Reporting

Employees are provided training on how to recognize suspected security incidents and where to report them. We utilize predefined and an exclusive communication channel to enable our employees to report any potential incidents. For relationships we have with external entities, they are informed of their responsibility to report information security events contractually.

SUPPLY CHAIN MANAGEMENT, TRANSPARENCY & ACCOUNTABILITY

Incident Reporting

As part of our incident response plan there are steps outlined to ensure all affected customers and providers are informed via electronic methods (ie - email).

Network/Infrastructure Services

We continuously monitor capacity and use data for all the relevant components of our cloud service offering. Additionally, we utilize automated procedures to increase compute resourcing, as needed to respond to increased capacity demands.

3rd Party Agreements

Our third-party agreements include provision for the security and protection of information and assets. We utilize cloud storage capabilities that are designed to reduce the likelihood of data loss and provide durability that is equivalent of multi-site copies.