SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Vendor is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between ESBOCES and Vendor to the contrary, Vendor agrees as follows:

Vendor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Vendor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Vendor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Vendor shall have in place sufficient internal controls to ensure that ESBOCES' and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or a Participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of ESBOCES and/or its Participants relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law 3012-c

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Vendor agrees to comply with ESBOCES policy(ies) on data security and privacy. Vendor shall promptly reimburse ESBOCES and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of ESBOCES' and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of ESBOCES' Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Vendor's policy on data security and privacy.

3. An outline of the measures taken by Vendor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how Vendor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how Vendor will ensure that any subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA SECURITY AND PRIVACY PLAN

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

An executed copy of ESBOCES' Parent's Bill of Rights is attached hereto and incorporated herein.

TEACHTOWN®

Exceptional Solutions for Exceptional Students

Technical and Security Overview

Version January 2024

TEACHTOWN®

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 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 v13 or greater
- Apps should work on all iPad models that support iOS 13. Older versions of iOS may work, depending on memory and CPU of the device
- 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.

SAML, SSO & 3rd Party Integrations

SSO/SAML

We offer SSO/SAML with Teachtown.com. More information on our SSO capabilities and setup are available in our guidelines here - SAML Single Sign On Integration (SSO) Guidelines.

OneRoster

We offer integration with OneRoster 1.1. More information on the OneRoster setup is available in our guidelines here - TeachTown OneRoster Integration Guideline.

Clever

We offer Clever SSO/Rostering for Teachers and Students with Teachtown.com. More information on Clever Setup is available in our guidelines here -
W Clever & TeachTown Integration Worksheet.docx

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer, New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

Student Data is used for the purpose of providing the district with the functionality of the products or services which is to provide teaching platforms for students in the K-12 environment.

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

Access to personally identifiable student data is managed by encryption, firewalls, password protection, disk encryption, file encryption and the NIST Cybersecurity Framework.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

Upon expiration of the contract, TeachTown will securely delete or otherwise destroy any and all Protected Data remaining in the possession of sub- contractors or other authorized persons or entities.

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

Complaints should be directed to the Associate Superintendent for Curriculum for your district; or in writing to: Chief Privacy Officer, New York State Education Department,
89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

Student personally identifiable information is stored in a secure, cloud environment located and deployed in Amazon Web Services and utilize Google Cloud storage capabilities across several geographically and logically separated locations.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Vendor hereby acknowledges that it is aware of and agrees to abide by the terms of this Bill of Rights. A copy of this signed document must be made a part of Vendor's data security and privacy plan.

SIGNATURE: Ashley Wall

NAME: Ashley Wall

TITLE: Chief Financial Officer