

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, ILLINOIS, MISSOURI, NEW HAMPSHIRE,
OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IL-MO-NH-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Hudson City School District

and

Spellzone Limited

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Hudson City School District, located at 76 N. Hayden Parkway, Hudson OH 44236 USA (the “**Local Education Agency**” or “**LEA**”) and Spellzone Limited, located at Holme Hill Cottage Church Street, Whixley York YO26 8AR, United Kingdom (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Barry Perks Title: Mr

Address: Holme Hill Cottage, Church Street, Whixley, York YO26 8AR UK

Phone: +44 333 990 013 Email: barry@spellzone.com

The designated representative for the LEA for this DPA is:

Stephanie Swiderski, Technology Coordinator

76 N. Hayden Parkway, Hudson OH 44236

330-653-1360 swiderss@hudson.k12.oh.us

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Hudson City School District

By: *Stephanie Swiderski* Date: 12/17/24

Printed Name: Stephanie Swiderski Title/Position: Technology Coordinator

Spellzone Limited



By: _____ Date: 17/12/2024

Printed Name: Barry Perks Title/Position: Mr/Director

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
- DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
- Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
- Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

- 1. Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
- 2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
- 3. Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
- 4. Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
- 5. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 6. Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
- 7. Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Spellzone, a browser-based, online English spelling program designed to support students in improving their spelling skills through interactive lessons, activities, and assessments.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	✓
	Other application technology meta data-Please specify: Google Analytics	✓
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	✓
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	✓
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify: See: Spellzone_Supporting_Notes_HudsonCity_OH_10State_NoNY_OHG_12-24.pdf	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify: Only if the school has created and organized students into a 'spelling intervention' group, 'dyslexia group' or similar.	✓
Student Contact Information	Address	
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify: Spellzone activity and results	✓
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C" DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	See: Spellzone_Supporting_Notes_HudsonCity_OH_10State_NoNY_OHG_12-24.pdf	
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"

Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."
2. Replace Notices with: "Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid."
3. In Article II, Section 1, add: "Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest."
4. In Article II, Section 2, replace "forty-five (45)" with "five (5)". Add the following sentence: "In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA."

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
10. In Article IV, Section 7, add “renting,” after “using.”

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA
as a result of the security breach; and
 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”

16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", "student temporary record" or "student permanent record" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA."

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E:
"The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”
Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	✓
	Other application technology meta data: Google Analytics	✓
Application Use Statistics	Meta data on user interaction with application	✓
Communications	Online communications that are captured (emails, blog entries)	✓
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email: Optional	✓
	Personal Phone: Optional	✓
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	✓
	Teacher app username	✓
	Teacher app passwords	✓
Teacher In App Performance	Program/application performance	✓
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify: Custom word lists	✓
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	






SpellZone_HudsonCity_OH_10State_NoNY_OH G_VendorSigned

Final Audit Report

2024-12-18

Created:	2024-12-18
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAVzgdIG-h1gJKpOzHqDgOaubhNpBsyod

"SpellZone_HudsonCity_OH_10State_NoNY_OHG_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-12-18 - 1:30:22 AM GMT
-  Document emailed to Stephanie Swiderski (swiderss@hudson.k12.oh.us) for signature
2024-12-18 - 1:30:35 AM GMT
-  Email viewed by Stephanie Swiderski (swiderss@hudson.k12.oh.us)
2024-12-18 - 2:38:49 AM GMT
-  Document e-signed by Stephanie Swiderski (swiderss@hudson.k12.oh.us)
Signature Date: 2024-12-18 - 2:40:30 AM GMT - Time Source: server
-  Agreement completed.
2024-12-18 - 2:40:30 AM GMT

- Note on Application Use Statistics - Meta data on user interaction with application: When students work from Spellzone material.
- Note on Enrollment: School can require students to complete the Spellzone Spelling Ability Test. This is a series of questions linked to Spellzone's course material and provides a baseline 'Spellzone Score' and a personal learning pathway for each student – it does not provide a spelling age.
- Note on Communications: Teachers can send pupils messages within Spellzone and allow pupils to respond to these. The communications are teacher > student/student > teacher only. These are only within the Spellzone environment (not by email). The Spellzone team can view and access these communications via the school account for support purposes.
- Note on Enrolment – Student School Enrolment/Grade Level: A school can choose to organize its students into classes for example Grade 4, Grade 5 etc. This is optional.
- Note on Student Contact Information – Email: Not mandatory. Only if uploaded by the school.
- Note on Student Identifiers – provider/App assigned student ID number: A unique identifier is created by Spellzone to identify their users for support purposes. These are not visible to the users.
- Note on Student app password: Created by the school or auto-generated by the Spellzone system. Passwords are not visible to Spellzone.
- Note on Student name: Only if a school has provided the full names of their students; alternatively, they can use only the initials of students or use other identifiers for example Student One, Student Two etc.
- Notes on Exhibit F Data Security Requirements - Adequate Cybersecurity Frameworks:
 - Spellzone is General Data Protection Regulation (GDPR) compliant: <https://gdpr-info.eu/>
 - Information Commissioners Office Registration. No. ZA004886.
 - Spellzone conforms to The Children's Code: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>
 - Cyber Essential Certified: <https://www.ncsc.gov.uk/cyberessentials/overview>
Certificate number: f7f85606-d78c-448b-ae24-9f308b3a5457
See attached: spellzone-limited_cyber-essentials_2024_certificate
 - EdTech Impact: Lawful, Ethical and Safe - 5 Star Certified:
<https://edtechimpact.com/products/spellzone/>
See attached report: Lawful, Ethical & Safe - Spellzone-3_27-11-24
- Notes on Exhibit K urls
 - Spellzone Data Sharing Agreement: <https://www.spellzone.com/pages/policies/data-sharing-agreement.cfm>
 - Spellzone Privacy Policy: <https://www.spellzone.com/pages/policies/privacy-policy.cfm>
 - Spellzone Child Friendly Privacy Policy: <https://www.spellzone.com/pages/policies/child-friendly-privacy-policy.cfm>
 - Spellzone Cookie Policy: <https://www.spellzone.com/pages/policies/cookie-policy.cfm>
 - Spellzone Terms and Conditions: <https://www.spellzone.com/pages/policies/terms.cfm>





CERTIFICATE OF ASSURANCE

Spellzone Limited

HGH (Spellzone), Club Chambers Museum Street York YO1 7DN

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Jason McWhirr

CERTIFICATE NUMBER : f7f85606-d78c-448b-ae24-9f308b3a5457

DATE OF CERTIFICATION : 2024-01-31

PROFILE VERSION : 3.1 (Montpellier)

RECERTIFICATION DUE : 2025-01-31

SCOPE : Whole Organisation



SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK




CERTIFICATION BODY



CYBER ESSENTIALS PARTNER



The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.



★ *edtech*
impact

Lawful, Ethical & Safe Evaluation

Spellzone 28.6.2024

About EdTech Impact

[EdTech Impact](#) provides an evidence-first marketplace that empowers educators and institutional leaders to make smarter buying decisions.

The platform brings together a diverse, and often siloed, community of EdTech users, EdTech providers, EdTech researchers and EdTech analysts to systematically assess the quality of education technology using a holistic assessment framework, global quality standards, and time-stamped certification programme.

Today, over 2,000 companies leverage the platform's data-driven insights to strengthen their product, showcase an independent and reliable evidence base, and gain access to a vibrant marketplace of over 400,000 in-market buyers.

EdTech Impact strikes a balance between robust research and practical user insights, giving a voice to all stakeholders, and an agile solution to building a sustainable evidence-first EdTech ecosystem within a variety of contexts.



The EdTech Impact Quality Framework is supported and governed by a consortium of research partners and expert organisations

About the EDDS Evaluation Method

EDDS provides evaluation across lawful, safe and security requirements to ensure children's fundamental rights, freedoms and needs are respected in digital learning environments based on its [methodology](#).

This report looks at minimum desired and appropriate to K-12 education needs and requirements achieved by Spellzone and makes recommendations as to what remedial actions could be taken to achieve a full digital certification of the product's lawfulness, safety and ethical soundness.

Evaluation Process

The evaluation process is straightforward and annual, supporting both the EdTech organisation's sustainability and growth, while simultaneously building trust in the education ecosystem - with schools, students, teachers, parents, policymakers, learning agencies, and other organisations and stakeholders caring for children.



About Spellzone

Spellzone is an online English spelling resource used by students aged six to adult. It unlocks the mystery of British English spelling and is adaptable for all abilities including SEND, SLD, ESL students and those with [dyslexia](#).

Data security contact

Barry Perks (Director)
admin@spellzone.com
03339 900132

Policy queries email address for customers

admin@spellzone.com

Compliance and Data Security

GDPR 2018 Compliance: Ensured

Data Encryption:

- In transit: Yes
- At rest: Yes
- Backups: Yes
- Portable devices: Yes

Policy Review Interval: Annually

User and Data Management

- Application uptime commitment: 99%
- Data retention period: 18 months
- Unique usernames and passwords: yes
- Role-based access control: yes
- Approved account creation: staff logins only created by existing staff members

Training and Screening

- Data protection training interval: annually
- Cyber security training interval: annually
- Employment screening (DBS): enhanced checks for staff

Third-Party and Cloud Services

- Customer data storage: within EEA
- Cloud Services: Bytemark, MailJet, YouCanBookMe
- Third-Party/Subcontractor Access to Data: No
- Third-Party Privacy Policies: Available upon request

Data Rights and Requests

- Right of rectification: through the school or direct request
- Right to erasure: through the school; data deleted as per retention policy
- Right to restrict processing: through the school or direct request
- Right of access: through the school or direct request
- Right to data portability: downloadable by the school
- Right to object: through the school

Security Features

- Protection against brute force attacks: yes
- All web services secured with trusted certificates: yes

Explanations



= *The compliance categories presenting the correct execution.*



= *The compliance categories presenting the most concern.*

Introduction	2
Data Responsibility and Privacy	8
Cybersecurity	24
Human Rights and Social-Ethical Aspects	32
Data Accessibility	35
Algorithmic Fairness	36
Summary of Findings	37

Data Responsibility and Privacy



Scope of the Privacy Policy



Highlights

- The Spellzone Privacy Policy fulfils the notification obligations overall and is written excellently to be clear and intelligible for the intended audience. That said, there are still a few recommendations that Spellzone can look into.
- Spellzone's Children-friendly Privacy Policy has provided additional information in a format aimed at a younger audience to address the Age Appropriate Design Code requirements.

Recommendations

- The Privacy Policy needs to be read in conjunction with the Terms & Conditions section of the website and the Data Sharing Agreement. Aspects relating to data protection, security and privacy were found in the T's & C's as well as the Data Sharing Agreement rather than in the Privacy Policy.
- Spellzone could boost its transparency and trust by referencing and linking additional compliance materials such as the Children's privacy policy, Cookie Policy, DPA put in place with third parties and security measures and certifications.

Action

- Conduct a thorough review of the Privacy Policy to ensure it accurately reflects valid consent mechanisms as per data protection regulations. Update the policy to align with legal standards and clearly communicate the lawful basis for data processing.
- Identify any data collected without proper consent and take corrective actions, such as obtaining valid consent or deleting non-compliant data.

Follow-up

- The above recommendations have been successfully addressed in the follow-up evaluation process.
- No further action is required.



Issues

- The lawful basis for processing has been stated more clearly.
- Spellzone has provide a clearer and more concise introduction that outlines the purpose of the section on lawful data processing and has demonstrated compliance with data protection laws.
- Additionally, following the audit evaluation, Spellzone has organized the introductory part to provide an overview of the lawful bases relied upon for processing personal data and added explicitly simple ways of how users may withdraw consent at any time without any negative ramifications.

Follow-up

- No further action required.

Useful Resources:

[Article 6 GDPR](#) list of applicable lawful bases.

Transparency



Highlights

- Overall, Spellzone has made tremendous efforts to provide transparency by undergoing all kinds of assessments and evaluation including with EDDS. Their Privacy Policy is understandable and well-suited to the intended audience. Concepts of processing are well explained including what personal data is, cookies, and what is done and not done with the data.
- The granularity of the data categories is excellent and well-structured.
- Overall, Spellzone has made tremendous efforts to provide transparency by undergoing all kinds of assessments and evaluation including with EDDS. Their Privacy Policy is understandable and well-suited to the intended audience. Concepts of processing are well explained including what personal data is, cookies, and what is done and not done with the data.
- The granularity of the data categories is excellent and well-structured.
- It would increase transparency to have a distinction between the lawful bases relied upon with the processing of different types of data.
- To improve transparency, additional information about the third parties engaged has been added and is useful.

Recommendations

- No further requirements necessary.

Follow-up

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Purposes of Processing



Issues

- While the different purposes of processing are mentioned throughout the privacy policy, they are not clearly outlined.
- Additionally, the screenshots provided that demonstrate the algorithmic functionalities (ranking, assessments, etc. of pupils' scores and other data and metadata) suggests that more detailed purpose of processing needs to be described. For example, what data points are used to create ranking and scoring.

Recommendations

- To fulfil transparency requirements around the purposes of processing, a section listing the purposes of processing should be added. Ideally, it should be clear to see what types of data are processed for what purposes. A table may be helpful to achieve this.

Action

- Create a dedicated section in the privacy policy that lists the purposes of processing, outlining each purpose clearly and specifying the types of data processed for each purpose. Utilize a table format to enhance clarity and organization, ensuring easy comprehension for users regarding the processing activities and associated data types.

Follow-up

- The above recommendations have been successfully addressed in the follow-up evaluation process.
- No further action is required.

Controllership



Highlights

- The controllership is clearly outlined throughout the documentation specifically of the Children's and Young People's Privacy Notice.
- Spellzone has boosted their transparency by providing a statement about controllership. Following the initial assessment by EDDS, Spellzone immediately incorporated a clear and concise statement about controllership in their privacy policy and the Children's and Young People's Privacy Notice.
- Spellzone has provided details around controllership responsibilities: a brief explanation of the responsibilities that come with being a data controller, including compliance with data protection laws, ensuring data security, and upholding data subjects' rights. This has enhanced users' understanding of the company's obligations and commitment to protecting their data, should controllership fall within Spellzone.

Recommendations

- No further requirements necessary.

Action

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Data Categories



Highlights

- The granularity of the data categories is excellent and well-structured.

Recommendations

- No further requirements necessary.

Action

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Data Sharing



Highlights

- Additional information has been provided that is listing why data may be shared with third parties, and what measures are in place to protect data shared.
- Notification obligations require controllers to list the categories of third-party data is shared with but this is not included in the Privacy Policy.
- Spellzone have included a list of the categories of third parties data that may be shared with accompanied by the purposes for data sharing.

Recommendations

- No further requirements necessary.

Action

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Data Automation, Profiling, Inferences, Use of Aggregated Data



Issues

- No detail is provided regarding how Spellzone achieves ranking and scoring, what data points are used (e.g., what user performance, activity, engagement and performance tracking data is used and how? What is the evidence to that [see further under **Additional Points**]).
- It would support the trustworthiness index of the company (using computation of scoring and any other algorithmic engagement), to explain clearly how such operations function. For instance, what frameworks or theories are the Spelling Ability Tests based on?
- There is no explicit information about how any aggregated data may be used.

Recommendations

- Special information need to be provided to address transparency around any algorithmic processing and computation relating to ranking, scoring and evaluation of the data (and which type) and the parties that may be involved in accessing, providing additional data and how such algorithmic data processing is used in decision-making.

Action

- Provide explicit detail about the algorithmic processing - is any occurring, what computation is being executed and what type of data is being used for such computation?
- List the parties that may be involved in the algorithmic data processing.
- Explain briefly how the algorithmic processing is used and in what ways - how decision-making may be affected.

Follow-up

- The above recommendations remain as future considerations should further advanced algorithmic or AI functionalities be introduced at the provider level. For the time being, the understanding is that basic computation is available both from user end and as a function of the product. Any inferential, predictive and other decision-making functionalities that may be deployed should be addressed and further examined from human rights and AI trustworthiness and fairness perspective.

Data Subject Rights



Highlights

- This section is very clear and well-explained in terms of the existing rights available and how a data subject can exercise their rights. Many privacy policies do not include information about the identification needed, this is excellent for transparency.

Recommendations

- No recommendations are needed.

Data Retention



Highlights

- This is clear regarding data processed under a trial or paid subscription.
- It is reassuring for data subjects to know data is only stored in the UK or EEA.

Recommendations

- There is no mention of the retention policy for personal data that is processed for purposes other than the trial or paid subscription. Suggestion to include information about the retention of other personal data.
- “Spellzone Limited will continue to store only the Personal Data needed after the contract has expired to meet any legal obligations after which it will be deleted, in a data-protection compliant manner.” - Which data and for how long? Additional details are needed to meet transparency requirements here.

Action

- Create a detailed data retention policy that outlines the retention periods for all categories of personal data processed by Spellzone, not just for trial or paid subscription data. Integrate this policy into the privacy policy.
- Specify retention periods for various types of data.
- Conduct periodic audits to verify that personal data is deleted in a data-protection compliant manner once the retention period expires.
- Don't forget to communicate any changes in the data retention policy to users promptly, ensuring they are informed about how their data is managed and protected.

Follow-up

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Withdrawal of Consent



Addressed action points

- The current privacy policy has adequately updated the issue of withdrawal of consent. The policy has updated their information on how users can withdraw their consent at any time and without negative consequences.
- The updated policy includes clear withdrawal procedure; the language used is easy to understand for users.
- No further actions are required.

Cookies



Highlights

- It is commendable that Spellzone does not engage with any advertising tracking technologies of concern. That said, there is only one interaction with the ad tracker **Alphabet, Inc.** No other trackers are detected on the page (after log-in to Spellzone) to be sending data to companies involved in online advertising. There are also no third-party cookies found, or tracking that evades cookie blockers, or Google Analytics or Facebook Pixel, or any methods of recording keystrokes, session recording services or similar.

Recommendations

- Nevertheless, Spellzone could still attend to the interaction its website makes with the ad tracker part of which is Google and associated companies like [Nest](#). The Silicon Valley giant collects data from twice the number of websites as its closest competitor, Facebook. Spellzone could provide some additional information for [opt out](#) of the company showing them targeted ads based on their browsing history.

Action

- Provide additional information about any ad tracker(s) the website may interact with, including opt out information.

Follow-up

The updated privacy policy and the Children and Young People

Additional Points (1)



Highlights

- Having a separate privacy policy directed at children is excellent. Nevertheless, additional information is needed and the format of the privacy policy information given could be improved and tailored better to children. As there are significant overlaps with the main Privacy Policy, please consider the following information:

Recommendations

- The Children's Privacy Policy appears to be a direct copy of the Privacy Policy with less information.
- Having a dedicated privacy policy for children presents an opportunity for Spellzone to demonstrate their understanding of the needs of children and build their trust. The tone, language and format used do not demonstrate any recognition of the different needs of children to provide them with an understanding of their data processed, the risks to them and the safeguards in place.
- Adjust the tone and language and consider using additional formats to explain concepts. Possible formats include icons, pictures and videos.

Action

- Specific action should be taken with regards to statements such as: “We ask all users under 18 to confirm they have permission from a parent or guardian before signing up”. Provide information about how and why you do this and how you ensure a parent or guardian is informed and in the loop.
- “Legal basis for processing your Personal Data” - This section does not provide any information about the legal bases used.
- It would be helpful to explain what a legal basis is e.g. what allows Spellzone to use data, and then explain what legal bases are used and why.

Follow-up

- A dedicated children and young people's policy is now available and no further actions are required.
- Additional information has been added with regards to the right to withdraw user consent. No further actions are required.
- Spellzone has also undergone EAF's assessment (see their [EdTech Impact profile](#)). No further actions are required.

Additional Points (2)

Issues

- Spellzone provides scoring, ranking, and other comparative and descriptive statistics; more analysis of these from pedagogical and algorithmic/computational perspective should be conducted.
- A mention of the DPO or contact details of the DPO are needed (if applicable). Given the intended audience, it is also recommended to briefly explain what a DPO is and does.
- It is recommended to have a contact email address of the Spellzone privacy specialist or DPO. Making requests by phone or post is not always the most convenient whereas email provides a good record of demonstrating compliance e.g. through data subject requests, general queries or complaints.

Recommendations

- It is crucial to assess such computations and descriptives to see their wider application and influence on decision-making. In this sense, Spellzone can engage with Edtech Impact's pedagogic framework (EAF) to evaluate the pedagogic value and impact on learning and decision-making.

Action

- From the screenshots of the platform, it looks as though teachers upload student data and have access to that data. This is not clear from the Children's Privacy Policy. This is something a child should know: what data their teacher uploads about them and what data they can see (e.g. names, user names, passwords, test scores).

Follow-up

- Spellzone have updated Children and Young People's policy which provides explicit information about their DPO and how they protect children's data and about the type of data that is being generated/provided access to. No further actions required.
- Spellzone are assessed across the EAF framework. No further actions required. See their [EdTech Impact profile](#).

Data Responsibility and Privacy Conclusion

Strengths:

Spellzone's efforts at privacy, lawfulness and safety are great.

1. The privacy policy is well-written and intelligible for the intended audience. This demonstrates significant effort in making data protection concepts accessible.
2. Spellzone demonstrates considerable strides in the efforts for transparency and accountability. The data categories are well-structured, and explained in an understandable manner.
3. Clarity around data storage in the UK or EEA is reassuring data subjects about locations where data privacy laws are strict and reliable.
4. The company does not use ad tracking technologies which demonstrates a dedicated focus on user privacy.
5. The use of local servers are also a star point; the company can physically visit their server locations and have additional oversight of their privacy and security commitments.

Cybersecurity



Security Hosting and Location



Highlights

- Spellzone has been certified by Cyber Essentials.

Issues

- There is no mention of what security measures are put in place. While this is not an essential requirement under the notification obligations, including security measures provides a way of reassuring data subjects and building trust in your services. Cyber Essentials, however, do not explicitly satisfy the unique needs and requirements of the educational domain.
- The company's hosting and third party provider is clearly stated in one of Spellzone's documentations. Their hosting provider is [Bytemark](#), iomart Group plc, 2 Opus Avenue, Poppleton, York, YO26 6BL with the following additional documentation: [Privacy policy](#), [Cookie policy](#), [Terms and Conditions](#)
 - iomart Group plc is approved by Icumus ISOQAR and is compliant with the
 - requirements of ISO 9001:2015. Certificate no: 7235-QMS-001 and the
 - requirements of ISO 27001:2013. Certificate no: 7235-ISMS-001. A Statement of
 - Applicability is available
- Spellzone's third-party email provider is [Mail Jet](#), 4 rue Jules Lefebvre, 75009 Paris. It tracks, monitors, and analyses email deliverability and customer engagement. And has the following additional documentation: [Privacy policy](#), [Cookie policy](#), [Terms and Conditions](#)

Recommendations

- It is suggested that the vendor is assessed across the Global Educational Cybersecurity Standard (GESS) framework which maps all major enterprise-level cybersecurity frameworks, including CE.

Action

- Link Data Security FAQs directly and explicitly with the Privacy Policy.
- Communicate any CE and other security assessments where all users can view, read and understand easily.

Useful Resources:

[GESS](#) framework

Encryption

Issues

- There is no knowledge if minimum encryption algorithms are applied to protect data in transit over public networks, etc.
- Wonde/third-party takes care of data access points, not Spellzone. This does not unburden Spellzone from the responsibility around data insecurities.

Recommendations

- While it may be the case that encryption is used at a minimum, it is recommended that leadership knows whether the product meets these standards.
- It is recommended that Spellzone are clear about the data access point and their practices around security standards, encryption and data privacy.

Action

- Provide explicit statement that the company is CE certified (year of issue) and what briefly this means in a language that is easy to understand.

Follow-up

- The above recommendations have been addressed. Additionally, these characteristics will be further amplified through EI's Manager functionalities.

Security Logging

Issues

- Spellzone have logs for every customer - the school and their admin is responsible to check logins.

Recommendations

- Provide clarity about how security logs on the customer side are maintained functional and safe or whether this responsibility is entirely exported to the client.

Follow-up

- No further actions necessary until changes of the scope, functionalities or other aspects of the software.

Security HR



Highlights

- Company staff has undergone DBS screening (two employees/company owner with advanced and one with standard DBS).
- It is commendable that the team of Spellzone under regular training and awareness.
- Data privacy policies and protocols for internal use are implemented across Spellzone's team. The following policies are implemented:

Recommendations

- Security training should be provided across several more aspects:
 - Children's rights
 - Safeguarding principles in an educational setting
 - Accessibility compliance policy (with regards to the EU Accessibility Act 2023)

Action

- Develop comprehensive Child's Rights Program. This video is a good start provided by EDDS: <https://www.youtube.com/watch?v=gYUjq-BUAeY>
- Provide training and education across fundamental child's rights and safeguarding principles and requirements.
- Maintain external audits and assessments that evaluate the effectiveness of these policies.

Data Privacy Policies and Protocols
Data Protection Policy
Privacy Policy and Child Friendly Privacy Policy
Subject Access Request Form
Subject Access Rights Policy and Procedure
Data Breach Notification Policy and Procedure
Data Protection Impact Assessment Policy and Procedure
Data Protection Impact Assessment
Data Protection Reporting Checklist
Data Security Policy
Register of Personal Data
Internal Data Breach Register
Processor Due Diligence Letter Template
Designated Contact Role and Responsibilities
Data Retention Policy
Data Retention Schedule
Data Sharing Agreement
Cookie Policy
Terms and Conditions
Staff Password Policy
Data Classification Standard
Data Handling Standards
Business Continuity and Data Breach Plan

Useful Resources:

Digital and technology standards for schools and colleges [DfE](#).

Encryption Algorithms Applied to Protect Data in Transit

Highlights

- School Data transfers are encrypted by the Spellzone website.

Issues

- Further information should be provided with regards to any cryptographic protocols that may be used such as SSL (Secure Sockets Layer) and TLS (Transport Layer Security). These are typically designed to provide secure communication over a computer network. TLS1.2 is a specific version of the TLS protocol.

Recommendations

- The SSL TLS 1.2 is an improved secure crypto protocol and is less vulnerable to cyber-attacks.

Action

- Update information at next external evaluation.

Security Plans and Quality

Report

Spellzone has a business continuity plan.

Recommendations

No further action required.

Security and Safety Result:

Strengths:

1. **Cyber Essentials certification:**
 - a. Spellzone is certified by Cyber Essentials, which demonstrates their commitment to implementing fundamental security measures to protect against common cyber threats.
2. **ISO 9001:2015 and ISO 27001:2013 compliance:**
 - a. Spellzone's hosting provider, iomart Group plc, is ISO 9001:2015 and ISO 27001:2013 certified. This compliance indicates that the provider follows international standards for quality management and information security management.
3. Clear documentation of third-party providers such as Bytemark for hosting and Mail Jet for email services, which allows extra transparency, while users can also reach out to these third party providers' privacy and cookie policies, terms and conditions.
4. **Staff screening and training** is noteworthy. Spellzone's staff undergoes DBS screening to ensure that employees handling sensitive data are vetted. Regular training and awareness programs are also in place which include data privacy policies and protocols.
 - a. Commitment to regular training and awareness is also one of the company's strengths.
5. Encryption of data transfers - school data transfers are encrypted by the Spellzone website, which ensures that data is protected during transmission.



Human Rights and Socio-Ethical Aspects

Not assessed/ Not applicable

Children's Rights



Issues

- Given the nature of the processing, it is certainly beneficial to include a section on the processing of children's data so this is good to see.

Recommendations

- The Children's Code is mentioned but there is no mention about what this is or where further information can be found.
- It would be useful to understand how the measures listed in the section 'Children's Data' are achieved e.g. "We try to avoid providing access links to any websites that request personal information, such as user email or physical addresses." - how is this done?
- Having a dedicated children's privacy policy is excellent but it is not mentioned or linked in the main privacy policy. A link to the Children's Privacy Policy should be given and accompanied by a statement such as "We have a dedicated Children's Privacy Policy to support children's awareness of the processing of their personal data".

Follow-up

- Spellzone has updated and provided additional clarification with regards to Children's Rights and thus acknowledging the importance of the Children's Code and how the functionalities of the application prioritises these.
- No further action is required at this stage until new functionalities or changes are made to the product.

Special Categories of Data



Highlights

- No special categories of personal data are listed.
- The mention in the Cookie section that no sensitive data is collected via cookies is good.

Recommendations

- Under the categories of personal data listed, a statement that no special/sensitive categories of personal data are collected would be useful to improve transparency and reassure data subjects.
- If specialist services are available to those with disabilities (e.g. visual impairments), then sensitive data may be inferred. If this is the case, it is suggested to mention this.

Action

- Enhance transparency in personal data categories: Include a specific statement under the categories of personal data listed in the privacy policy, explicitly stating that no special or sensitive categories of personal data are collected. This addition will improve transparency and reassure data subjects about the nature of the data collected.

Follow-up

- The new Children and Young People's Privacy policy details definitions around personal data and that no special categories data is collected. The policy also clearly defines what data is collected in plain and child-friendly language. No further action required.

Useful Resources:

[Article 9\(1\) GDPR](#) provides a list of special categories.

See a [Guide and checklist](#) to processing special categories lawfully.



Algorithmic Fairness

Not assessed/ Not applicable

Summary of Findings

Spellzone's dedication to security, transparency and privacy are commendable.

Best features:

1. **Clarity and understandability:** The Privacy Policy is well-written and clear for the intended audience, which demonstrates the company's dedication to enhancing transparency and trust.
2. **Data subject rights explanation:** The section on Data Subject Rights is comprehensive and transparent, providing clear guidance on how users can exercise their rights.
3. **Children's Privacy Policy:** Having a dedicated policy for children demonstrates a commitment to their privacy, though improvements are needed.
 - **DPIAs and Cyber Essentials:** Spellzone is assessed across various frameworks, and requirements, and has been certified and showing excellence and full commitment to transparency and accountability.



Summary of Findings

Overall, while Spellzone demonstrates good clarity and coverage of the key statutory areas, enhancements in consent management, transparency, and the children's privacy policy are vital for compliance and building trust with their users. Several aspects can also be considered going forward:

Areas for improvement, which have, following the audit and evaluation, been met. The below are kept for audit and transparency records.



1. **Consent management:** There is a critical need to improve consent management, ensuring it aligns with GDPR requirements, and users can easily manage their consent preferences. **Follow-up: this is now completed. No further action required.**
2. **Age-Appropriate designs:** While Spellzone does not fall within the category of an ISS (information society services), the company has been self-assessed against ICO's Children's Code and have a DPIA in place for all development work. **No further action is required.**



For more information:

hello@edtechimpact.com

edtechimpact.com