Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

TESTIMONY TO THE VERMONT HOUSE COMMERCE COMMITTEE
RE: H.650 - Educational Technology Products

Submitted by: Jeff Wallis, Director of Technology and Network Engineering
Mount Mansfield Unified Union School District
Date: February 6, 2026

Dear Members of the Commerce Committee,

I am writing to provide testimony on H.650, a bill relating to educational technology products. As the Director of Technology and Network Engineering for Mount Mansfield Unified Union School District, I appreciate the legislature's attention to student data privacy and security. I share the goals of this legislation and want to offer insight from our district's experience with educational technology and student data privacy to help inform your deliberations.

CURRENT STUDENT DATA PRIVACY PRACTICES

What is the Vermont Student Privacy Alliance (VTSPA)?

Our district is a member of the Vermont Student Privacy Alliance (VTSPA), which was established in 2018 as a collaboration of Vermont supervisory unions and school districts that share common concerns around student privacy. Membership in the Vermont Student Privacy Alliance is free to Vermont school districts, courtesy of the Vermont Agency of Education (AOE). The AOE is an official partner of the Student Data Privacy Consortium, and Vermont districts may join and use the database of negotiated agreements at no cost to individual districts.

The national Student Data Privacy Consortium and Vermont's state partnership with them ensures that our schools have free access to:

- The SDPC Resource Registry (a database of executed agreements)
- Model Data Privacy Agreements (DPAs)
- Training and support resources
- A community of other schools addressing data privacy

This standardization means that vendors and schools have common expectations when entering into relationships without having to renegotiate terms in every instance.

Since 2016, over 275,000 standard Data Privacy Agreements have been executed and subscribed to nationally through this consortium, demonstrating the widespread adoption and effectiveness of this approach.

The way the agreement process works:

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

1. The originating district uses a model data privacy agreement and this is then signed by the district and the vendor
2. Subscribing districts can also sign an “exhibit e” agreement, which then also gives them the same protections and agreement as the originating district
3. The data privacy agreement is then added to the database for all other members to view

This makes it easy to enter into agreements for schools and vendors. This is important because it keeps the costs down for new software and agreements can be created in a timely manner

While VTSPA membership is free, our district invests an additional $1 per student per year by contracting with the Technology and Education Cooperative (https://tec-coop.org/data-privacy/). This is a non-profit entity. This service provides our district with several critical functions:

1. Drafting and negotiating comprehensive Student Data Privacy Agreements with vendors
2. Managing and maintaining these agreements - constantly monitoring vendor changes to terms of service, data breaches, changes to software, etc.
3. Holding vendors accountable to their contractual obligations
4. Providing expertise in data privacy law and best practices (all contracts are reviewed by their lawyers)

I have attached one of our student data privacy agreements for your review for Corel Vector.

This agreement includes:
• Detailed definitions of student data and how it may be used
• Strict limitations on data collection (only what is essential for educational purposes)
• Prohibition on selling or sharing student data with third parties
• Requirements for encryption and data security measures aligned with NIST Cybersecurity Framework
• Parent access rights to review and correct student data (within 45 days)
• Data breach notification procedures (within 72 hours)
• Provisions for data disposal upon contract termination (within 60 days)
• Compliance with FERPA, COPPA, and state-specific privacy laws for Vermont
• Restrictions on targeted advertising and student profiling
• Annual security audits (with 10 business days' notice)
• Criminal background checks for employees

This agreement is notable because it covers design and graphics software used in our middle schools for design tech classes. Despite being general-purpose design software not specifically created for education, this company operates under the same strict contractual limitations that protect student privacy. Under the definition of the bill, I believe they would be considered an educational provider. I am not sure if they would submit to a certification process to prove they

provide an educational program even though this is a valuable learning tool for our students. This is just one example of many software tools that we use for education that may not consider themselves ed tech software.

I would also like to add that we require a student data privacy agreement for all software that collects student data. This is not limited to only student facing software.

OUR CURRENT VETTING PROCESS

When a teacher requests new educational software, we follow a multi-step evaluation process:

1. Initial Request: Teachers complete a software request form which includes questions such as:
   - What is the content goal or task that you want students to accomplish?
   - How will this tool help you accomplish your learning goals for students?
   - What specific features does this tool offer that other tools don't offer?

2. Privacy Review: We determine whether we can negotiate a data privacy agreement through the student data privacy consortium

3. Educational Review: Our curriculum coaches, digital learning leaders and curriculum counsels work with the teachers to evaluate whether the software meets educational requirements and aligns with our curriculum standards

4. Financial Analysis: We review the cost and assess whether we have similar tools already in our technology portfolio, part of this includes the cost of supporting the software and professional development

5. Pilot Program: If the software passes all these hurdles, we conduct a pilot program with a limited group of teachers and students to assess its effectiveness

6. Full Implementation: After a successful pilot, we make the software available to all students at the appropriate grade level - this ensures consistency and equity across the district

This process ensures both data privacy protection and educational quality while being fiscally responsible. Importantly, by going through this comprehensive educational software vetting process, we ensure that there is genuine buy-in to using the software. The teachers and curriculum leaders who will be using these tools with their students have made the professional determination that the software supports the student learning outcomes. This teacher-driven approach means that software adoption is purposeful and pedagogically sound.

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

While our district has implemented strict data privacy procedures, I acknowledge that not all Vermont school districts have the same level of oversight. This disparity is a legitimate concern that H.650 seeks to address. As you consider this legislation, I'd like to share some observations about implementation that may be helpful.

As you refine H.650, I'd like to highlight some areas that may benefit from further discussion:

1. Scope and Definition of Educational Technology

The bill defines "educational technology product" as "any student-facing software, application, or platform that may collect, process, or transmit student data and that is used for teaching and learning purposes in a school."

This definition would encompass a wide range of tools. To help illustrate the scope, here are examples of commonly-used platforms in our schools:

- Google Workspace for Education (including Docs, Sheets, Slides): Students use these to create writing assignments, presentations, and collaborative projects. Google Docs processes and stores student-generated content.
- Learning Management Systems: Schoology, Google Classroom
- Video editing software: such as WeVideo
- Educational Content Platforms: Renaissance Learning, Happy Numbers, MathFacts Lab
- Design and Graphics Software: Tools like CorelDRAW Graphics Suite used in visual arts, graphic design, and middle school design technology classes

These tools range from general-purpose platforms to specialized educational software. Questions to consider: Would all of these require state certification? How would the certification process handle multi-product vendors like Renaissance Learning, which offers assessment, practice, and data analytics tools? Would they need separate certifications for each product, or would a vendor-level certification be sufficient?

The bill's current certification criteria include things like:
"Compliance with State curriculum standards"
"Advantages of using the product compared with nondigital methods"
"Whether the product was explicitly designed for educational use"

These criteria make sense for purpose-built educational software like Renaissance Learning's Star Assessments, but become harder to apply to general-purpose tools like Google Docs (which wasn't designed specifically for education but is used extensively for student writing) Some general purpose tools may not pursue certification or meet these requirements. Would we then not be able to use these tools with students?

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

2. Implementation and Resource Considerations

Section 2 of the bill requires schools to submit a list of all educational technology products currently in use by December 15, 2026. To provide context, our district uses over 110 different software tools and platforms across all grade levels and subject areas. Across Vermont's 300+ schools, this represents a significant collective effort. More importantly, the Secretary of State's office would need resources to review and certify potentially thousands of products. Does their office have the resources to chase down and monitor certification in a timely manner?

Understanding the resource implications for both schools and the state may be helpful in planning for implementation of this bill.

3. Certification Standards and Process

The bill gives the Secretary of State authority to "develop, publish, and annually review the standards for the certification."

- Does the Secretary of State's office have expertise in educational technology, curriculum development, and pedagogy. Will they partner with the AOE? Would a task force or work group be created for this work?
- How would the Secretary of State ensure certification criteria can be applied consistently across diverse products? Would professional educators be involved? Many ed tech vendors include their own studies of educational effectiveness in their marketing packages yet still do not align with our local curriculum goals. Does their study outweigh our professional educators evaluations?
- Will the July 1, 2027 timeline be achievable to evaluate and process potentially 1000s of software tools? And will it give schools enough time to adapt their curriculum?
- This bill calls for an annual review of standards. This could affect multi-year contracts between schools and vendors. Many of our purchase contracts span 3 or even 5 years to save money and reduce annual increases. Would we continue to pay for these resources but not be able to use them if they didn't certify? Would we be forced to have annual contracts, thus increasing our costs?

4. Data Collection Requirements

This bill specifies that the vendor will not collect "demographic data of a student except for the name and grade level of the student". Some software we use does collect demographic data for valuable data analysis by our educators.

4. Cost Considerations

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

The bill requires providers to register annually with the Secretary of State ($100 fee) and establishes penalties up to $10,000 for failure to register, along with a state certification review process.

It's worth considering that these costs may be passed through to schools in the form of higher software prices. For smaller educational technology companies, Vermont-specific registration and certification requirements may affect their ability to serve Vermont schools, potentially reducing vendor options for our schools.

APPROACHES TO CONSIDER

Building on the existing Vermont Student Privacy Alliance framework, here are some approaches that could work for H.650's implementation:

1. District-Level Software Vetting Procedures

Consider requiring all Vermont school districts to implement and document procedures for vetting educational technology products. These procedures could include:

- Review of vendor data privacy and security practices
- Evaluation of educational value and curriculum alignment
- Cost-benefit analysis
- Pilot testing before full implementation

The state could provide a model policy for districts that included required components

2. Leveraging the Existing Vermont Student Privacy Alliance

The Vermont Student Privacy Alliance already has established requirements that meet the state certification standards:

- Compliance with FERPA, COPPA, and Vermont privacy laws
- Prohibition on selling student data
- Restrictions on data collection to only what is necessary for educational purposes
- Encryption of data in transit and at rest
- Data breach notification procedures
- Parent/guardian access rights
- Data deletion upon contract termination
- Prohibition on targeted advertising to students
- Annual security assessments

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

This bill could mandate the use of model data privacy agreements through the Vermont Student Privacy Alliance. This would include the use of the vendor agreements inventory in the Student Data Privacy Consortium database that is already funded by the AOE. It could include the funding for privacy review services for all districts ($1 per student through the Technology and Education Cooperative (https://tec-coop.org/data-privacy/) or similar services.

3. Vendor Accountability Mechanisms

To ensure vendor compliance, consider establishing requirements for vendors to:

- Sign Vermont Student Privacy Alliance compliant agreements
- Notify districts of any material changes to their data practices
- Provide transparency reports on data breaches and security incidents

SUPPORTING TEACHING AND LEARNING

As you consider implementation timelines and scope, it may be helpful to understand how teachers currently use technology in classrooms to:

• Differentiate instruction for diverse learners
• Provide immediate feedback to students
• Enable project-based and collaborative learning
• Support students with special needs
• Engage digital-native learners
• Prepare students for a technology-driven workforce

Ensuring continuity of access to these tools during any transition or certification period would help maintain instructional quality and avoid disruption to student learning.

CONCLUSION

Keeping our students safe is critically important, and I commend the spirit of this bill.

As you refine the legislation, I hope this testimony has been helpful in highlighting:

- Some of the potential issues with the certification process done by the Secretary of State's office
- The robust privacy infrastructure that already exists through the Vermont Student Privacy Alliance (free to all districts through AOE partnership)
- How comprehensive data privacy agreements currently work in practice while also highlighting the need for all districts to adopt these practices
- The vetting process for educational technology and how it is working in our schools, with a need for all schools to understand and follow a similar process

Mount Mansfield Unified Union School District
10 River Road Jericho, VT 05465
P:802-434-2128 F:802-899-4001
districtoffice@mmuusd.org
www.mmuusd.org

I would be happy to provide additional information about our district's data privacy practices, share our template agreements, discuss implementation details, or serve as a resource to the committee in any way that would be helpful.

Thank you for your dedication to keeping our students safe and for considering this testimony.

Respectfully submitted,

Jeff Wallis
Director of Technology and Network Engineering
Mount Mansfield Unified Union School District
10 River Rd, Jericho, VT 05465
802-434-2803
jeff.wallis@mmuusd.org

STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND, AND VERMONT

MA-ME-NH-RI-VT-NDPA, Standard Version 1.0

MOUNT MANSFIELD UNIFIED UNION SCHOOL DISTRICT

and

Corel Corporation

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: Mount Mansfield Unified Union School District, located at 10 River Rd, Jericho, VT 05465 (the "**Local Education Agency**" or "**LEA**") and Corel Corporation, located at Corel Corporation (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: Grant Parsamyan Title: Chief Information and Data Officer

Address: 700-333 Preston Street, Ottawa, Canada, K1S 5N4

Phone: (613) 728-8200

Email: privacy@alludo.com

The designated representative for the LEA for this DPA is:

Jeff Wallis, Director of Technology and Network Engineering
Mount Mansfield Unified Union School District
10 River Rd, Jericho, VT 05465
802-434-2803
jeff.wallis@mmuusd.org

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

MOUNT MANSFIELD UNIFIED UNION SCHOOL DISTRICT

By: Jeff Wallis (Jun 12, 2023 09:33 EDT)

Date: 6/12/2023

Printed Name: Jeff Wallis

Title/Position: Director of Technology

Corel Corporation

By:

Date: May 25, 2023

Printed Name: Grant Parsamyan

Title/Position: Chief Information and Data Officer

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **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

2. **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"**.

3. **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

1. **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.

2. **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.

3. **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.

4. **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

CorelDRAW Graphics Suite
CorelDRAW Standard
CorelDRAW Technical Suite
Corel Vector
CorelCAD

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.	Yes
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	Yes
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:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Name	First and/or Last	
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:	
Student Contact Information	Address	
	Email	Yes
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	Yes
	Student app passwords	Yes
Student Name	First and/or Last	Yes
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.	Yes
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	

Category of Data	Elements	Check if Used by Your System
	Student pick up and/or drop off location	
	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**]

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

2. Nature of Disposition

__x___ 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:

_x___ As soon as commercially practicable.

_____ By [**Insert Date**]

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

May 25, 2023

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Mount Mansfield Unified Union School District** ("Originating LEA") which is dated 6/12/2023, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following **email address:** privacy@alludo.com.

Corel Corporation

BY: _____ Date: May 25, 2023

Printed Name: Grant Parsamyan Title/Position: Chief Information and Data Officer

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **Mount Mansfield Unified Union School District** and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA: (School District Name): _____

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	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"
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"
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"
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.	Yes
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	Yes
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	Yes
	Personal Phone	
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	Yes
	Teacher app passwords	Yes
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	Yes
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Corel_MountMansfield_VendorSigned

Final Audit Report 2023-06-12

Created:	2023-06-12
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAa4sEBO9tWC1N1F2PkhpVzNF9a6NK3nRa

"Corel_MountMansfield_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2023-06-12 - 1:24:28 PM GMT- IP address: 108.35.203.7

Document emailed to Jeff Wallis (jeff.wallis@mmuusd.org) for signature
2023-06-12 - 1:25:18 PM GMT

Email viewed by Jeff Wallis (jeff.wallis@mmuusd.org)
2023-06-12 - 1:32:36 PM GMT- IP address: 73.182.223.226

Document e-signed by Jeff Wallis (jeff.wallis@mmuusd.org)
Signature Date: 2023-06-12 - 1:33:30 PM GMT - Time Source: server- IP address: 73.182.223.226

Agreement completed.
2023-06-12 - 1:33:30 PM GMT