

**WISCONSIN STUDENT DATA PRIVACY AGREEMENT**

**School District/Local Education Agency:**

**Steven Point Area Public School district**

**AND**

**Provider:**

**EXPERT SOFTWARE APPLICATIONS SRL (MINDOMO)**

**Date: Jan 18, 2022**

This Wisconsin Student Data Privacy Agreement (“DPA”) is entered into by and between the [Insert Name] (hereinafter referred to as “LEA”) and [Name of Company] (hereinafter referred to as “Provider”) on [Insert Date]. The Parties agree to the terms as stated herein.

## **RECITALS**

**WHEREAS**, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a contract dated [Insert Date] (“Service Agreement”); and

**WHEREAS**, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to Wisconsin state student privacy laws, including pupil records law under Wis. Stat. § 118.125 and notice requirements for the unauthorized acquisition of personal information under Wis. Stat. § 134.98; and

**WHEREAS**, for the purposes of this DPA, the Provider is a school district official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

**WHEREAS**, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other LEAs in Wisconsin the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

## **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 transmitted to the Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and applicable Wisconsin law, all as may be amended from time to time. In performing these services, the Provider shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, the Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:

[Insert Brief Description of Products and Services]

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”.

[Insert Categories of Student Data to be provided to the Provider]

4. **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 term used in the Service Agreement.

## **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 Agreement 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 District Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. The Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. The Provider shall respond in a timely manner (and no later than 30 days from the date of the request) to the LEA’s request for Student Data in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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 pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, the Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact the Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. The Provider shall notify the LEA as soon as possible in advance of a compelled disclosure to a Third Party.

### ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Annual Notification of Rights.** The LEA shall include a specification of criteria under FERPA 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 data.

4. **Unauthorized Access Notification.** LEA shall notify the Provider promptly of any known or suspected unauthorized access. LEA will assist the Provider in any efforts by the Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF THE PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. The Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation.** The Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure.** The Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, the Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any student data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes the Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. The Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement the Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, the Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall the Provider dispose of data pursuant to this provision unless and until the Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** The Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. The Provider is also prohibited from mining data for any purpose other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is

prohibited. This section does not prohibit the Provider from using Student Data for adaptive learning or customized student learning purposes.

## ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of the Provider are set forth below. The Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** The Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. The Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** The Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes the Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. The Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, the Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, the Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. The Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

**f. Security Coordinator.** If different from the designated representative identified in Article VII, section 5, the Provider shall provide the name and contact information of the Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

**h. Periodic Risk Assessment.** The Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

**2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, the Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. The Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
  - 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 because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
  - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA's discretion, the security breach notification may also include any of the following:
  - i.** Information about what the agency has done to protect individuals whose information has been breached.
  - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.



- d. The Provider agrees to adhere to all requirements in applicable state and federal law 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.
- e. The 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 copy of said written incident response plan.
- f. The Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests the Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to the Provider, the Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, the Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, the Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

#### **ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS**

The 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

#### **ARTICLE VII: MISCELLANEOUS**

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.
2. **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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

**a. Designated Representatives**

The designated representative for the LEA for this Agreement is:

**Name:** Brian Casey  
**Title:** Director of Technology  
**Contact Information:**  
[bcasey@pointschools.net](mailto:bcasey@pointschools.net)

715-345-7393

The designated representative for the Provider for this Agreement is:

**Name:** Nadina Barzeianu  
**Title:** Sales and Communications Coordinator  
**Contact Information:**  
[nadina.barzeianu@exswap.com](mailto:nadina.barzeianu@exswap.com)  
+40 256 486 430

- b. Notification of Acceptance of General Offer of Privacy Terms.** Upon execution of Exhibit "E", General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for notice of acceptance of the General Offer of Privacy Terms is:

Name: Nadina Barzeianu

Title: Sales and Communications Coordinator

**Contact Information:**

[nadina.barzeianu@exswap.com](mailto:nadina.barzeianu@exswap.com)

+40 256 486 430

8. **Entire Agreement.** This DPA constitutes 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.
9. **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.
10. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WISCONSIN, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
11. **Authority.** The Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. The Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

12. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
13. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to the 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 WITNESS WHEREOF**, the parties have executed this Wisconsin Student Data Privacy Agreement as of the last day noted below.

Provider:

BY: EXPERT SOFTWARE APPLICATIONS SRL Date: Jan 18, 2022

Printed Name: NADINA BARZEIANU  
Title/Position: SALES AND COMMUNICATIONS COORDINATOR

Local Education Agency:

BY:  Date: 1-18-2022

Printed Name: Brian Casey Title/Position: Director of Technology

## **EXHIBIT “A”**

### **DESCRIPTION OF SERVICES**

- yearly Mindomo School package for as many teacher and student accounts needed
- both teachers and students will benefit from fully premium accounts
- unlimited mind maps, concept maps, and outlines, with real-time collaboration
- teachers can create [mind map assignments](#), allowing students to work individually or in groups to create mind maps. The students' progress becomes instantly available to the teacher, who can give them grades and real-time feedback
- LTI integration with the most popular LMS tools (Canvas, Moodle, Schoology, Desire2Learn, itslearning, [Blackboard](#))
- integrations with Google Classroom, G Suite, Office 365, Google Drive, MS Teams
- premium access to the Desktop app (Windows, Mac, or Linux) with the possibility to synchronize maps between desktop-cloud versions
- Android and iOS mobile apps with the possibility to synchronize maps between mobile-cloud versions
- Automatic license assignment mechanism: people who sign up to Mindomo using emails with the board's domains will be automatically added to the Mindomo license and given premium accounts.
- Educational templates - partially filled in structures containing instructions that facilitate the creation of mind maps
- Multiple export formats: PNG, TXT, HTML, PDF, DOCX, OPML, MPX, XLS, ZIP, PPTX
- Playback of the mind map/assignment history: an overview of all map changes, which illustrates the contribution of each person who works on the map
- Presenter mode: turning mind maps and concept maps into a slide by slide presentations
- Advanced customization options and personalization of the maps with multimedia (video, audio, images)

**EXHIBIT “B”**

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	YES
	Other application technology metadata - 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 that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred 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	YES
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
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	
	Vendor/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:	Mindomo diagrams with all related attachments
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	
	Student bus card ID number	
Other	Please list each additional data element used, stored or collected by your application	



## **INFORMATION WE COLLECT**

Mindomo collects the following information about you and your use of our Service:

### **Personally Identifiable Information**

- The following personal information is gathered when a user registers:
  - first and last names
  - email address
  - password
  - age
  - parent email address for users who are less than 13 (United States) and 16 (European Union) years of age. All student data are securely maintained, used only for educational purposes, and not shared with any other organizations.
- Upon setting up their Mindomo Profile, the user may optionally provide the following personal information:
  - a profile photo
  - username
  - a URL to a website
  - short text about the user
- In addition to the information we collect when the user registers or sets up his/her Mindomo Profile, we may ask for additional personal information at other times, such as when the user makes a purchase on our website, and contacts our technical support team.
- Furthermore, when the user sends an email or other communication to Mindomo, we may retain those communications in order to process the user's inquiries and requests and to improve our services.

### **Personally Identifiable Information from Integrated Services**

If the user decides to register through or otherwise grant access to a third-party social networking or integrated service, Mindomo will collect the following personal information that is already associated with the user's integrated service account:

**Facebook:** id, email, first name, last name

**Yahoo:** id, email, first name, last name

**Windows Live:** id, email, first name, last name

**Office 365:** id, email, first name, last name

**Clever:** id, email, first name, last name, account type

**Google:** id, email, first name, last name and any personal info you've made publicly available

**SamI:** email, last name, first name

**LTI:** email, last name, first name

If the user chooses to provide such information, during registration or otherwise, the user is giving Mindomo the permission to use, share, and store it in a manner consistent with this Privacy Policy.

### **Information Collected at Purchase**

Purchases are made through the [Braintree](#) and [2Checkout](#) online payment providers. When a user purchases one of our products, we ask for the standard and necessary information required for user identification and processing of the transaction.

At present, the information collected during the purchase process includes user's account information (full name, email, password) and billing information (name, country, VAT ID where applicable, address, city, ZIP code, state/province, telephone number) and sufficient credit card information (number, expiry date, name on card, CVC) to authorize the transaction with the card provider.

When a user purchases one of our products, we automatically add their invoice, along with all the above information, to our database for future communication about the purchased product (updates, fixes, enhancements), and, according to the law, tax preparation, tracking expenditures and overall business budgeting. Invoices will be kept during the entire statute of limitations for when the tax records can be changed or reviewed.

At no time will the user's personal information nor purchase information (including credit card information) be sold, rented, or revealed in any way to a third party. We will not use the information provided for any purpose other than record-keeping purposes and communicating about the purchased products in the most efficient way possible.

### **Location Information**

We collect the IP address you use to connect to the Service and — if you choose to share it — your location information from a mobile device but we don't collect the precise geolocation of you or your device. You may be able to change the settings on your computer or mobile device to prevent it from providing us with any location information.

### **Integration with optional third party Services**

#### **YouTube**

By using the integrated YouTube search functionality and embedding YouTube videos to your Mindomo documents (mind maps, concept maps, Gantt charts, outlines, etc.) through the YouTube API Services, you also acknowledge and agree to the connected use of the Google

Privacy Policy <https://www.google.com/policies/privacy> and the YouTube terms of service <https://www.youtube.com/t/terms>

## **Vimeo**

By using the integrated Vimeo search functionality and embedding Vimeo videos to your Mindomo documents (mind maps, concept maps, Gantt charts, outlines, etc.), you also acknowledge and agree to the connected use of the Vimeo privacy policy <https://vimeo.com/privacy> and the Vimeo terms of service <https://vimeo.com/terms>

## **Bing**

Mindomo's integrated image search functionality is powered by Bing. By choosing to use the integrated image search functionality and embed images to your Mindomo documents (mind maps, concept maps, Gantt charts, outlines, etc.), you also acknowledge and agree to the Microsoft Services Agreement <https://www.microsoft.com/en/servicesagreement/> and the Microsoft Privacy Statement <https://privacy.microsoft.com/en-us/privacystatement>

By choosing to add attachments to your Mindomo documents from a cloud storage account or to use our options of backup to these accounts, you also acknowledge and agree to these services' terms of service: [Dropbox](#), [Google Drive](#), [OneDrive](#).

By using the option to add notes to your Mindomo documents through our Evernote integration you also acknowledge and agree to the to the Evernote Terms of service <https://evernote.com/legal/terms-of-service> and Evernote Privacy Policy <https://evernote.com/privacy/policy>

## **HOW WE USE THE INFORMATION WE COLLECT**

The information users submit to us is primarily used for their account creation and generally used for carrying out user requests, processing orders, responding to inquiries, better serving users or in other ways naturally associated with the circumstances in which the users provided the information.

When a user is using our Service and is asked for personal information, the user is sharing that information exclusively with us, unless it is specifically stated otherwise. From time to time, we may use information collected to provide the user with feedback or to communicate about the Service's latest improvements and updates.

## **HOW WE SHARE THE INFORMATION WE COLLECT**

Some of our users choose to connect their Mindomo accounts with social networks. This functionality is entirely optional. If the user has explicitly agreed that we may do so, Mindomo may disclose the part of the collected user's personal information (first and last name) through a social network or similar service (like Facebook or Google).

Mindomo may also disclose user information if required to do so by law, or if we have a good-faith belief that such action is necessary to comply with local, state, federal, international, or other applicable laws or respond to a court order, judicial or other government subpoenas, or warrant, or administrative request. In some cases, we may make such disclosures without first providing notice to users.

Mindomo will not disclose any of the user's personally identifiable information to third parties except when we have the user's permission or under specific circumstances, such as when we believe in good faith that the law requires it. The following describes some of the circumstances under which your information may be disclosed.

Mindomo is using the services of two data centers, both of which are ISO/IEC 27001 certified (The ISO 27001 certificate, an internationally recognized standard for information security). The main data center is Hetzner Online GmbH, located in Germany. The second data center is Amazon, located in Ireland, where Mindomo does regular backups.

As we continue to develop our business, we may sell or purchase assets. If Mindomo becomes involved in a merger, acquisition, or any form of sale of some or all of its assets, the user's personal information may be transferred to the purchaser. If another entity acquires us or all (or substantially all) of our assets, the personally identifiable information and non-personal information we have about the user will be transferred to and used by this acquiring entity, provided the successor entity is subject to the same commitments for the previously collected user information. No personal information will be transferred in the event of a merger or sale unless the recipient has committed to our Privacy Policy. In such an event, Mindomo will always notify the user before the information is transferred.

Mindomo may disclose information that we believe, in good faith, is appropriate or necessary to take precautions against liability; to protect Mindomo from fraudulent, abusive, or unlawful uses; to investigate and defend ourselves against any third-party claims or allegations; to assist government enforcement agencies; to protect the security or integrity of our properties; or to protect the rights, property, or personal safety of Mindomo, our users, or others.

## **HOW WE COLLECT AND USE NON-PERSONAL INFORMATION**

Like most websites and online services, Mindomo automatically collects usage information when a user visits our website or otherwise engages with us. This information is typically collected through a variety of tracking technologies, including cookies, log files, and similar technology (collectively, "tracking technologies"). These tracking technologies collect information about the user's visit to the website (e.g., viewed pages, links clicked) and online usage patterns (e.g., Internet Protocol ("IP") address, browser type, browser language, referring/exit pages and URLs, pages viewed, whether the user opened an email, links clicked).

We may collect analytics data to help us measure traffic and usage trends for the website and to understand more about the demographics of our users.

We do not permit third parties to collect information from our website for the purpose of sending targeted advertisements on our site or on other websites.

We use or may use the data collected through tracking technologies to better display our website, to save our users' time, to provide better technical support, and to track website usage.

Most browsers are initially set up to accept cookies, but users can reset their browsers to refuse all cookies or to indicate when a cookie is being sent.

## EXHIBIT “C”

### DEFINITIONS

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

**Educational Records:** Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

**NIST:** Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

**Operator:** The term “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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

**Personally Identifiable Information (PII):** The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of the Provider’s software, website, service, or app, including mobile apps, whether gathered by the Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

**Provider:** For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Pupil Generated Content:** The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education 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 pupil content.

**Pupil Records:** Means all of the following: (1) Any information that directly relates to a pupil that is maintained by LEA;(2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee; and any information that meets the definition of a “pupil record” under Wis. Stat. § 118.125(1)(d). For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

**Service Agreement:** Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

**School District Official:** For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B) and Wis. Stat. § 118.125(2)(d), a School District 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 education records; and (3) Is subject to 34 CFR 99.33(a) and Wis. Stat. § 118.125(2) governing the use and re-disclosure of personally identifiable information from student records.

**Student Data:** Student Data includes any data, whether gathered by the 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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Wisconsin and federal 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 the Provider’s services.

**SDPC (The Student Data Privacy Consortium):** Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

**Student Personal Information:** “Student Personal Information” means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies

an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

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

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**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 pupil records. However, for the purpose of this Agreement, 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

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

<p><b><u>Extent of Disposition</u></b></p> <p>Disposition shall be:</p>	<p>_____ Partial. The categories of data to be disposed of are as follows:</p> <p>_____ Complete. Disposition extends to all categories of data.</p>
<p><b><u>Nature of Disposition</u></b></p> <p>Disposition shall be by:</p>	<p>_____ Destruction or deletion of data.</p> <p>_____ Transfer of data. The date shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, the Provider shall destroy or delete all applicable data.</p>
<p><b><u>Timing of Disposition</u></b></p> <p>Data shall be disposed of by the following date:</p>	<p>_____ As soon as commercially practicable</p> <p>_____ By (Insert Date) _____</p> <p>[Insert or attach special instructions]</p>

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

\_\_\_\_\_  
Verification of Disposition of Data  
by Authorized Representative of the Provider

\_\_\_\_\_  
Date



**EXHIBIT “E”**

GENERAL OFFER OF PRIVACY TERMS  
[INSERT ORIGINATION LEA NAME]

**1. Offer of Terms**

The Provider offers the same privacy protections found in this DPA between it and [Name of LEA] and which is dated to any other LEA (“Subscribing LEA”) who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and the Provider’s signature shall not necessarily bind the 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 other LEA may also agree to change the data provided by LEA to the Provider in Exhibit “B” to suit the unique needs of the 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 subject listed in the Originating Service Agreement; or three (3) years after the date of the Provider’s signature to this Form.

Provider:

BY: EXPERT SOFTWARE APPLICATIONS SRL Date: Jan 18, 2022

Printed Name: NADINA BARZEIANU Title/Position: SALES COORDINATOR

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with the 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.

Subscribing LEA:

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

**TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW**

Name: NADINA BARZEIANU

Title: SALES AND COMMUNICATION COORDINATOR

Email Address: [nadina.barzeianu@exswap.com](mailto:nadina.barzeianu@exswap.com)

**EXHIBIT “F”**

DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENT]