ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

STUDENT DATA PRIVACY AGREEMENT

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Brisk Labs Corp. ("Service Provider" or "Vendor") on 07/11/2025 ("Effective Date").

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

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed, or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms; and

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

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Agree

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems, including file servers, routers, switches, NDS, and Internet services, is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software, is prohibited.

   Agree: Agree

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code, and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Agree

Provider Initial: ML
Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage, or use for demonstration purposes any Roseville City School District data without the prior written consent of Educational or Technology Services management.

   Agree: Agree

5. **TRANSPORT**: The Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Agree

6. **EXTERNAL SECURITY:** The Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Agree

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personnel (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protect unauthorized access to District data? How are backups performed, and who has access to and custody of the backup media? How long are backups maintained? What happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard-copy records?

   Agree: Agree

8. **DISTRICT ACCESS:** The Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Agree

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. The Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Agree

Provider Initial: ML
Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

Provider Initial: ML

Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Agree

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

   Agree: Agree

3. Vendors cannot sell student information.

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

Provider Initial: ML

Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section IV: Audit and Compliance Oversight

1. **Audit Rights.** The District reserves the right to audit the Vendor's privacy and security practices no more than once annually or at any time in response to a data incident, suspected noncompliance, or legal/regulatory inquiry. The Vendor shall provide reasonable access to systems, records, and personnel involved in the handling of District data.
2. **Confidentiality Agreement.** RCSD agrees to execute a reasonable non-disclosure agreement to protect Vendor trade secrets or proprietary information disclosed during the audit.

Section IV: Audit and Compliance Oversight (*Continued*)

3. **Framework Compliance.** Vendor agrees to implement and maintain security controls consistent with one or more of the following frameworks:
    a. NIST Cybersecurity Framework (NIST CSF)
    b. NIST SP 800-53 or 800-171
    c. ISO/IEC 27001
    d. CIS Critical Security Controls (Top 18)

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

    Designated Security Framework(s):
    NIST Cybersecurity Framework (NIST CSF)

4. Security Program Documentation. Upon request, the Vendor shall furnish RCSD with the following:
    a. A summary of its data security policies and incident response procedures.
    b. Results from the most recent third-party security assessment or audit, redacted as necessary.
    c. Any certifications (e.g., SOC 2, ISO 27001).
5. **Remediation Obligations**. If a security deficiency or compliance failure is identified, the Vendor shall deliver a written remediation plan to RCSD within thirty (30) days. The District may suspend access to its data until the deficiency is addressed to the District's satisfaction.
6. **Subprocessor Oversight**. The Vendor is responsible for ensuring that all subprocessors or affiliates with access to District data comply with the terms of this agreement and are subject to equivalent audit and compliance obligations.

Provider Initial: ML
Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

Here is Brisk's Network Security Policy, which outlines our use of firewalls, intrusion detection systems (IDS), and other layered security controls to protect our systems from external threats and unauthorized access - https://drive.google.com/file/d/18DtQiGv2-oFYD3cQjKwoW-uchQquww7G/view?usp=drive_link

Section 1.7: Internal Security

Data Processing and Storage: Brisk processes district data in secure cloud environments, utilizing vendors like AWS and Microsoft Azure. Data is stored and accessed in compliance with security policies, ensuring that it is protected at all times.
Access Control: Access to district data is strictly controlled and granted only to authorized personnel, based on a need-to-know basis, to fulfill contractual obligations. This access is monitored and logged.
Data Encryption: District data is encrypted both at rest (when stored) and in transit (when transferred), following Brisk's Encryption Policy, ensuring data security during storage and while being exchanged between systems.
Backup and Data Deletion: Our product is hosted on Amazon Web Services (AWS), which provides secure, redundant infrastructure. We use AWS services to perform automated backups of critical systems and data at least weekly—or more frequently depending on data sensitivity. Recovery data is protected with equivalent controls to the original data, referencing encryption or data separation based on requirements. Stored sensitive data that is no longer required will be properly deleted in accordance with Brisk Teaching's business objectives, retention policies, applicable laws and regulations, and relevant third-party agreements. A record of such deletion will be kept. Hard-copy materials with sensitive data will be destroyed when no longer needed for business or legal reasons through secure means (e.g., shredding, pulping, incinerating, etc.) so that the data cannot be reconstructed. Hard copy materials will be stored in secure storage containers prior to destruction.
Internal Security Policies:Brisk has internal policies to prevent unauthorized access or misuse of district data. Access to the data is limited to personnel who have a legitimate business need.

Section II.2: Exporting of Student-Created Content

Student created work can be exported upon request by reaching out to privacy@briskteaching.com.

Provider Initial: ML
Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

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

Brisk Teaching has processes to correct erroneous information. Requests from parents or students will be redirected to the District. Individuals using Brisk on behalf of a district may email privacy@briskteaching.com to challenge the accuracy of data.

Section II.5: Securing Student Data

Here is our Data Processing Addendum, which how outlines how Brisk ensures the security and confidentiality of student data: https://www.briskteaching.com/brisk-data-processing-addendum

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

Here is our Privacy Notice, which describes how Brisk and its third-party affiliates comply with FERPA requirements - https://www.briskteaching.com/privacy-notice

Section III.5: How Student Data is Protected:

Here is our Data Processing Addendum, which outlines the reasonable security procedures and practices Brisk Teaching uses to protect student information -- https://www.briskteaching.com/brisk-data-processing-addendum

Provider Initial: ML

Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

1. AI Usage Limitations and Ownership

1.1. The Service Provider shall not use or reproduce Student Data for Artificial Intelligence (AI) training, model development, or content generation without the District's prior written consent. The Provider agrees to uphold the principles outlined in California Education Code §33328.5, ensuring that any AI systems used in connection with the Service align with values of equity, safety, transparency, and accountability in the interest of student welfare.

1.2. Sub-licensing Student Data for such purposes is strictly prohibited unless explicit written permission is obtained from the student's parent, legal guardian, or eligible student.

1.3. Ownership of all Student Data, including content generated with AI assistance, remains with the District or the student, as applicable.

2. Notification and Consent

2.1. If any feature of the Service is modified to include AI functionality, the Provider shall notify the District in writing prior to deployment.

2.2. The Provider must disclose the types of AI used, the purpose of such use, and how Student Data will be processed within these features.

2.3. No AI feature may be enabled until the District provides written consent and has reviewed any updated data-handling practices.

3. Algorithm Bias and Fairness

3.1. The Provider certifies that any AI technologies used in facilitating the Services are regularly audited for algorithmic bias and fairness.

3.2. Upon request by the District, the Provider shall furnish a summary of audit findings related to bias detection and mitigation strategies. These audits shall demonstrate the Provider's commitment to promoting equitable outcomes and addressing systemic bias, as emphasized in California Education Code §33328.5(d).

4. AI Hallucinations and Reliability

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

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

Provider Initial: ML
Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

5. Prohibited Uses of AI

5.1. The Provider shall not:

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

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

6. Student Content and AI-Generated Work

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

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

7. Transparency and Disclosure Requirements (SB 942)

7.1. The Provider shall maintain and make publicly available a free tool that enables users to verify whether content was generated by AI. This tool shall:

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

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

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

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

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

Provider Initial: ML
Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

8. Definitions

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

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

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

9. Compliance with State Advisory Guidelines

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

Provider Initial: ML
Date: 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

DATA INCIDENT NOTIFICATION ADDENDUM

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

1. Data Incident Notification

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

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

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

2. Notification to Affected Individuals and Authorities

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

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

2.1.1. Be written in plain language;

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

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

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

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

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

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

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

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

2.2.6. Steps the individual can take to protect themselves.

Provider Initial: ML

Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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

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

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

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

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

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

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

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

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

Provider Initial: ML
Date: 07/11/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

3. **Legal Compliance and Risk Management**

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

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- State-specific data breach notification statutes

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

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

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

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

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

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

Provider Initial: ML

Date 07/11/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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

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

Service Provider		**Roseville City School District**	
Maryel Ley		Laura Assem	
Authorized Representative Signature		*Authorized Representative Signature*	
Date:	07/11/2025	**Date:**	07/14/2025
Name:	Maryel Ley	**Name:**	Laura Assem
Title:	Head of Operations	**Title:**	Executive Director, Technology
Email:	privacy@briskteaching.com	**Email:**	lassem@rcsdk8.org

Privacy Notice

***Effective Date**: 04/14/2025* | Previous Version

This Service Privacy Notice applies to the products and services of Brisk Labs Corp. ("Brisk," "we," "our," or "us") that link to this page, such as Brisk's online platforms and web browser extensions (collectively, our "Service"). We maintain a separate Website Privacy Notice for visitors to the briskteaching.com website.

Through our Service, we provide productivity tools that speed up tasks like lesson planning and grading, engage student learning, and more. This Privacy Notice describes how we 1) collect, use and disclose your personal data as a controller when you use our Service or otherwise engage with us, and, 2) how we process personal data in our role as a processor when our Service is used by providers of educational services, such as schools and school districts (collectively, "Schools"), as well as teachers and authorized school users and administrators (collectively, "Educators").

When the Service is used as part of a School's educational curriculum, the personal data related to students ("Students") that is (i) provided to Brisk by a School, or (ii) collected by Brisk during the provision of the Service to a School, may include information defined as "educational records" by the Family Educational Rights and Privacy Act ("FERPA"), "covered information" under California's Student Online Personal Information Protection Act ("SOPIPA"), "personal information" under Canadian provincial and territorial privacy legislation, or other information protected by similar data privacy laws. We call this information "Student Data." The School is the controller of Student Data, and we handle Student Data in our role as a processor on behalf of the School. If you are a Parent or Student and have questions about specific practices relating to Student Data provided to Brisk by a School, please direct your questions to your School.

Please see the "Student Data" section below to understand the principles which guide our collection, use and disclosure of Student Data.

For more information about our product available for students, please refer to our disclosures for Brisk Boost, below.

*If you are an Educator who will use the Service in an educational setting, and your School has not entered into a separate student data processing agreement with Brisk, please note that the **Brisk Student Data Processing Addendum** applies to your use of the Service.*

TABLE OF CONTENTS

1. WHAT IS PERSONAL DATA?

In short: "Personal data" means data or information that identifies or relates to you, or otherwise meets the definition below.

When we use the term "personal data" in this Privacy Notice, we mean any data or information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular natural person or household.

2. OUR COLLECTION OF PERSONAL DATA AS A CONTROLLER

In short: We collect personal data in the ways described below. For example, we may collect personal data when you register for an account on our Service, send us messages, subscribe to our mailing lists, participate in a survey, or integrate our Service with a third-party site or service. In addition, we may collect personal data automatically when you interact with our Service. We may also collect personal data about you from other sources and third parties.

Information You Provide

We collect the following information you provide in connection with our Service:

- **Account Information**, including full name, email address, School name, and other account information that you choose to provide to us.
- **Inquiry and Communication Information,** including information you provide to us when you submit a form, email us, or call us regarding our Service.
- **Information Collected Through the Use of the Service**, including any files, documents, videos, images, or other information you choose to provide through your use of the Service.
- **Information from Educators**, such as School name, district, teacher or authorized administrator title, organizational units associated with the School, course information and topics, grade levels taught, course work and assignments, course sections.
- **Student-related Information**, such as topics of study, assignments and content (e.g., homework), and grades. For more information about our privacy practices with regard to Student Data, please see the **Student Data** section below.

Personal Data Automatically Collected

We and our third-party providers may use (i) cookies or small data files that are stored on an individual's computer and (ii) other, related technologies, such as web beacons, pixels, embedded scripts, location-identifying technologies and logging technologies (collectively, "cookies") to automatically collect certain data regarding how you interact with our Service, such as log files and analytics data. For more information about how we use cookies and your choices regarding cookies, please see our **Cookie Notice for the Service.**

Personal Data from Third Parties

We also obtain personal data from third parties. We often combine with personal data we collect either automatically or directly from an individual. We may receive the same categories of personal data as described above from the following third parties:

- **Information That Our Users Direct Us to Process**: We may receive your information from other users who interact with our Service. For example, if an Educator uses our browser extension's Inspect Writing feature, our Service will process any personal data included in the document. For more information about how we use information that our users direct us to process, please see our **Privacy and Security FAQs**.
- **Referral Information**: We may receive your contact information from people who think you may also be interested in our Service. For example, an Educator may provide us with your contact information as a part of a referral program.

- **Information We Receive from Third-Party Platforms**: Some parts of our Service allow you to login or link your account with a third-party platform, such as Google. These platforms give you the option to share certain personal data with us that you make available on those platforms. For example, if you register through or otherwise link your Brisk account with your Google account (e.g., Google Classroom, G-Suite including Google Docs, Google Chrome, and Google Drive), we may collect personal data that is associated with your Google account. This information we collect may include your name, account profile data, email address, courses, Student rosters, course materials, information about Google Doc views, version history, comments, and authentication action information, and Student submissions, including some Student Data. If you create or upload assessments or other academic or educational resources or materials from a linked third-party platform, we collect the content of these materials and metadata you provide about them. Our Service's use and transfer of information received from Google APIs to any other app will adhere to **Google API Services User Data Policy**, including the Limited Use requirements.
    - The information we receive from a third-party platform depends on the third party's policies and your privacy settings on its platform. You should always review and, if necessary, adjust your privacy settings on third-party platforms before linking them to our Service.

- **Other Sources**: We may also collect personal data about individuals that we do not otherwise have from, for example, publicly available sources, third-party data providers like MDR, or through transactions such as mergers and acquisitions.

3. OUR USE OF PERSONAL DATA

In short: We use personal data to manage our organization and its day-to-day operations. For more details, please see below:

We use personal data to:

- Verify your identity and check whether you are permitted to access certain features of our Service.
- Provide our Service. For example, as part of our 'Inspect Writing' feature, Brisk accesses the version history of documents.
- Personalize our Service, including by recognizing an individual and remembering their information when they return to our Service.
- Conduct research and analytics on our user base and our Service.
- Send communications, including via email and newsletters.
- Improve and customize our Service to address the needs and interests of our user base and other individuals we interact with.
- Test, enhance, update and monitor the Service, and diagnose or fix technology problems.
- Help maintain the safety, security and integrity of our Service, technology assets and other property, and our business.

- To enforce our contractual rights, to resolve disputes, to carry out our obligations and enforce our rights, and to protect our business interests and the interests and rights of third parties.
- Prevent, investigate or provide notice of fraud or unlawful or criminal activity.
- Comply with contractual and legal obligations and requirements.
- To fulfill any other purpose for which you provide personal data.
- For any other lawful purpose, or other purpose that you consent to.

We never sell personal data from our Service. We also do not share personal data from our Service with third parties for their own marketing purposes. Our Service is free from any advertising, ensuring a secure, distraction-free educational environment for both Students and Educators. For example, we do not use third-party cookies on our Service for personalized advertising or to track users and display personalized advertisements on other third-party websites or services.

Where you choose to contact us, we may need additional information to fulfill the request or respond to inquiries. We may provide you with additional privacy-related information where the scope of the inquiry/request and/or personal data we require fall outside the scope of this Privacy Notice. In that case, the additional privacy notice will govern how we may process the information provided at that time.

4. OUR DISCLOSURE OF PERSONAL DATA

In short: We disclose personal data to a few different categories of recipients. Recipients may include companies that enable us to provide AI-powered services, your School, and others as described below.

We may also share, transmit, disclose, grant access to, make available, and provide personal data with and to third parties, as follows. For more information on how we share Student Data that we collect from Schools, including a list of the specific third parties with whom Student Data is shared, please see the section on "**Student Data**" below.

- **AI Service Providers:** We share personal data with service providers who enable us to provide AI-powered services. For example, this may include service providers who assist us in providing the AI-powered tools that form a part of our Service. Our current list of service providers is available upon request. As required by applicable data protection laws, we impose contractual limits on how these service providers can use the personal data they receive.
- **Other Service Providers:** We also share personal data with our other service providers, such as vendors who help us with data analysis, fraud prevention, infrastructure provisioning, analytics services, IT services, product fulfillment, and web hosting. Our current list of service providers is available upon request. As required by applicable data protection laws, we impose contractual limits on how these service providers can use the personal data they receive.

- **Your School:** If you interact with our Service through your School, we may disclose your information to your School.

- **Other Users**: Our Service does not currently enable users to post public profiles. However, if you are a member of a Slack channel, Facebook group or other online community group relating to our Services, your public profile information for the applicable online community group will be disclosed to other members of that online community, as well as any other information you choose to provide or make public.

- **Customer Service and Communication Providers:** We share personal data with third parties who assist us in providing customer service and facilitating our communications with individuals that submit inquiries. As required by applicable data protection laws, we impose contractual limits on how these third parties can use the personal data they receive.

- **Business Transaction or Reorganization**. We may take part in or be involved with a corporate business transaction, such as a merger, acquisition, joint venture, or financing or sale of company assets. We may disclose personal data to a third party during negotiation of, in connection with or as an asset in such a corporate business transaction. Personal data may also be disclosed in the event of insolvency, bankruptcy, or receivership. As required by applicable data protection laws, we impose contractual limits on how applicable third parties can use the personal data they receive.

- **Legal Obligations and Rights**. We may disclose personal data to third parties, such as legal advisors and law enforcement:
    - in connection with the establishment, exercise, or defense of legal claims.
    - to comply with laws or to respond to lawful requests and legal process.
    - to protect the rights and property of Brisk, our agents, users, and others, including to enforce our agreements, policies, and **terms of service**.
    - to detect, suppress, or prevent fraud.
    - to reduce credit risk and collect debts owed to us.
    - to protect the health and safety of us, our users, or any person.
    - as otherwise required by applicable law.

- **With Your Consent or At Your Direction**. In addition to the sharing described in this Privacy Notice, we may share information about you with third parties whenever you consent to or direct such sharing.

When we disclose personal data to third parties, we take steps to protect the data in a manner that is consistent with our policies and obligations under applicable privacy laws.

5. STUDENT DATA

In short: We consider Student Data to be confidential and do not use Student Data for any purpose other than to provide the Service on the School's behalf, in accordance with our contract with the School. For more details about our Student Data privacy practices, please see below.

To help Schools address their obligations to protect their students' data privacy, we have implemented additional controls and procedures for Schools when they enter into a contract with Brisk to use the Service as part of a School's educational curriculum, such as Brisk's Student Data Privacy Addendum or another similar set of protections requested by the School. When the Service is used as part of a School's educational curriculum, the personal data related to Students that is (i) provided to Brisk by a School, or (ii) collected by Brisk during the provision of the Service to a School, may include information defined as "educational records" by the Family Educational Rights and Privacy Act ("FERPA"), "covered information" under California's Student Online Personal Information Protection Act ("SOPIPA"), "personal information" under Canadian provincial and territorial privacy legislation, or other information protected by similar data privacy laws. We call this information "Student Data."

- As between us and the School, Student Data is owned and controlled by the School. Our collection and use of Student Data is in our role as a processor and is governed by our agreements with the Schools and by applicable privacy laws. For example, we provide the Service to Schools as a "School Official" under FERPA
- We collect, maintain, use and share Student Data only for an authorized educational purpose and as described in our agreement with the School, or as directed by the School or by the Student's parent or legal guardian (each, a "Parent").
- We do not use or disclose Student Data for targeted advertising purposes.
- We do not build a personal profile of a Student other than in furtherance of an educational purpose.
- We maintain a comprehensive data security program designed to protect the types of Student Data maintained by the Service. For more information about our security practices, please see the **Security** section below.
- We will clearly and transparently disclose our data policies and practices to our users.
- We will never sell Student Data unless the sale is part of a corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets, in which case we will require the new owner to continue to honor the terms provided in this Privacy Notice or we will provide the School with notice and an opportunity to opt-out of the transfer of Student Data by deleting the Student Data before the transfer occurs.
- We will not make any material changes to our Privacy Notice or agreements that relate to the collection or use of Student Data without first giving notice to the School and providing a choice before the Student Data are used in a materially different manner than was disclosed when the information was collected.

How We Share and Disclose Student Data

- We disclose Student Data solely as needed to provide the Service on behalf of specific Schools in accordance with our agreements with those Schools or with the consent of the School or Parent.

- For example, Student Data and account usage data may be disclosed to or accessible by users who are authorized to use the Service on behalf of the School, for example a school or district administrator. In addition, depending on the manner in which Brisk is used by the School and the terms of the agreement between the School and Brisk, we may provide access to certain Student Data to the Student and/or to the Parent of the Student about whom the data relates, for the purpose of monitoring Student usage and activity and evaluating the effectiveness of the School's use of the Service.

- We also disclose Student Data to trusted service providers who have a legitimate need to access such information on our behalf, subject to appropriate contractual terms to protect such data. Our current list of service providers is available in Schedule 4 of our Data Processing Addendum.

We may also disclose Student Data in connection with a business transaction or to support our legal rights and obligations, as described in the **Our Disclosure of Personal Data** section of this Privacy Notice.

How We Use De-Identified Data

Where permitted by law and in accordance with our agreements with Schools, we may also generate, use, and disclose de-identified information for adaptive learning purposes or customized student learning purposes, to recommend content or services relating to School purposes or other educational or employment purposes, as well as for development, research and improvement of our Service. In addition, we may use de-identified information for the development and improvement of other educational sites, services and applications or technologies more generally to the extent permitted under applicable law. "De-identified information" means data from which all personally identifiable information has been removed or obscured so that the remaining information does not reasonably identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

How We Retain Student Data

We will not knowingly retain Student Records beyond the time period required to support an educational purpose, unless authorized by the School.

Please note: Schools are responsible for maintaining current class rosters, and for managing Student Data which they no longer need for an educational purpose by submitting a deletion request.

If you are using the Service on behalf of a School and wish to access Student Data, delete Student Data or close your account, please contact us (**privacy@briskteaching.com**). If you are a Parent or

Student and wish to access Student Data, delete Student Data or close your account, please direct your request to your School.

Questions About Student Data

If you are a Parent or Student and have questions about specific practices relating to Student Data provided to Brisk by a School, please direct your questions to your School.

6. CHILDREN'S PRIVACY - BRISK BOOST

In short: We may choose to make parts of our Service available to children under 13 years old, such as Brisk Boost. Our privacy practices with regard to children under 13 are set out below. We will not collect personal data from children under 13 without appropriate consent or authorization.

In addition to our tools for Educators, our **Brisk Boost** offering provides a powerful tool designed to help learners boost their academic progress using AI.

We may choose to make Brisk Boost available to children under the age of 13. However, Brisk will not collect personal data from children under 13 without appropriate consent or authorization, as follows:

- When Brisk provides the Service on behalf of a School, the School provides consent for Brisk to collect information from Students under the age of 13 through the Service provided on the School's behalf, as permitted by the Children's Online Privacy Protection Act ("COPPA") and other applicable data privacy laws. In this case:
    - We collect and process personal data from Students under 13 solely at the direction of and under the control of a School, and do not require Students to disclose more information than is reasonably necessary to use the Service.
    - At all times, Schools have the right to request to review or delete the personal data from Students under 13 or decline to permit further collection or use of the Students' personal data by contacting the School's account representative.
    - Schools are responsible for providing appropriate notice to Parents of the School's use of third-party service providers such as Brisk. We recommend that our School customers provide a link to this Privacy Notice to all Parents.
    - For more information on how we collect and process Student Data, please see the section on **Student Data** above.
- When Brisk provides the Service directly to children under 13 outside of the school context, we require the child's parent or legal guardian to provide the appropriate consent or authorization for their child to use Brisk.
- The parent, legal guardian or school may withdraw consent at any time.

Data Collected from a Child

When a child under 13 uses the Service, we will ask for certain information about the child that is typically provided by the adult setting up the Service for the child, which may include the child's name and information about the child's parent, guardian or School (as applicable).

When the child uses the Service, we will collect the following information from the child:

- Information Collected Through the Use of the Service, including any files, documents, videos, images, or other information the child chooses to provide through the child's use of the Service.
- Student-related Information, such as topics of study, assignments and content (e.g., homework), and grades.
- Usage information, such as date/time of visit, time spent on our Service, time zone, and activities completed or engaged with through the Service.
- Device data and log files, which could include IP address, operating system, device type and version, browser type and version, browser id, and location data derived from IP address. This information is typically collected through cookies or similar technologies and we may use third-party providers to collect this information on our behalf. We collect this information to help us understand usage, to diagnose problems and provide support, to administer our Service, facilitate navigation, display information more effectively, to remember users' settings and preferences, to personalize the user's experience while using the Service, and to recognize a user's computer or device in order to assist the use of the Service and for security purposes.

We do not require the child to provide any more information than is reasonably necessary to use the Service.

How we share or disclose a child's personal data

We share or disclose a child's personal data as needed to provide our Service or with third parties with appropriate consent or authorization. For example, we share a child's personal data with third parties as authorized by the Parent or the School, such as school administrators, counselors, resource professionals and others subject to appropriate authorization. Similarly, children may communicate with others through the Service subject to appropriate authorization, such as with their teachers. Brisk Boost users are not permitted to interact with other untrusted users.

We also share information with our trusted third-party service providers who provide services to us or on our behalf, such as website hosting and customer support services, information technology and related infrastructure provision, and other services.Our current list of service providers is available in Schedule 4 of our Data Processing Addendum. As required by applicable data protection laws, we impose contractual limits on how these service providers can use the personal data they receive.

We may also share personal data if we believe to be necessary or appropriate: (a) under applicable law; (b) to comply with legal process; (c) to respond to requests from public and government

authorities, including public and government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety or property, and/or that of our affiliates, our users or others; and (g) to allow us to pursue available remedies or limit the damages that we may sustain. If Brisk becomes involved in a merger, acquisition, bankruptcy, change of control, or any form of sale of some or all of its assets, a child's personal data may be transferred or disclosed in connection with the business transaction, subject to any applicable laws.

We may also share aggregate or de-identified information in a manner that cannot be reasonably used to identify an individual user.

How to access and delete a child's personal data

A parent/guardian has the right to access the personal data we have collected from the child, withdraw consent for further collection and request deletion of the child's personal data. If you are a Parent of a child under 13 that uses our Service outside of school and you want to access, correct, or delete your child's personal data, please contact us to submit your request. If you are a Parent of a Student under 13 using the Service through a School and you want to access, correct, or delete the Student's personal data, please contact your child's School to submit your request. We will respond to the School's instructions with respect to your child's personal data.

Unless we receive a deletion request, we will retain the personal data collected from the child for as long as necessary to provide the Service and comply with our legal obligations, which could include retaining information as needed for recordkeeping and billing obligations. We will delete and/or de-identify the child's personal data when it is no longer needed for the purposes for which it was collected.

If you require additional assistance regarding your child's personal data, please contact us at **privacy@briskteaching.com**. We will respond to all requests as soon as possible. For requests that relate to Students, we may be required to refer the request to the School or School administrator for action.

If you believe a child under the age of 13 has provided personal data to us other than as described above, please contact us using the information in the Contact Us section below so that we may delete such information.

7. YOUR PRIVACY CHOICES

In short: If you would like to update, access, review, modify or delete your information you can do so as described below.

You may control your information in the following ways:

- **Profile, controls and data sharing settings**. You may update your account information and may change some of your account controls and data sharing preferences by visiting your "Account" page, removing our browser extension via the "settings" or "tools" menu on your web browser, or emailing us at **privacy@briskteaching.com**.

- **Disconnecting your Brisk account from third party sites**. As discussed above, you may be able to connect your Brisk account to accounts you have on third party sites such as Google. You may disconnect your account from a third-party site at any time by visiting the "Account" page to remove authenticated sites and services or removing the Google Chrome Extension under the "Tools" page.

- **Changing your cookie preferences**. For additional details about the cookies we use on our websites and to adjust your preferences with regard to those cookies, please review our **Cookie Notice for the Service.**

- **Changing your communications preferences**. You can stop receiving promotional email communications from us by clicking on the "unsubscribe link" provided in such communications. We make every effort to promptly process all unsubscribe requests. You may not opt out of service-related communications (e.g., account verification, transactional communications, changes/updates to features of the Service, technical and security notices).

- **Accessing, reviewing, modifying or deleting your information**. If you want to access, review, modify or delete your information, or if you want to remove your name or comments from our Service or publicly displayed content, you can contact us directly at **privacy@briskteaching.com** to submit your request. We will respond to these types of requests in compliance with any applicable data protection laws.

8. SECURITY

In short: We maintain technical and organizational safeguards for personal data as described below.

Brisk has a multi-tiered approach to protecting personal data that includes technical and organizational safeguards. Brisk enforces a robust security program comprised of policies and controls aimed at protecting personal data against known and anticipated threats. Brisk's security controls include, for example, firewalls, role-based access controls, and encryption. Our technical and organizational security controls are described in more detail in **our Data Processing Addendum**.

Brisk restricts access to personal data to a need to know basis and maintains a disciplinary process for any violations.

For Schools that provide us with a designated point of contact for security breaches, Brisk maintains a Student Data breach response protocol. In the event of unauthorized access, destruction, use, modification, or disclosure of Student Data, designated points of contact at Schools will be notified by email or other direct communication channels in accordance with the protocol.

We process and store personal data in the United States and other jurisdictions where our service providers are located. Please be aware that your personal information could therefore be accessed by law enforcement agencies, courts and other governmental authorities in those jurisdictions. Contact us using the contact information provided below if you have questions about our use of service providers.

9. CONTACT US

In short: Please feel free to contact us with any questions. Our contact info is below.
If you have any questions or requests in connection with this Privacy Notice or other privacy-related matters, please send an email to **privacy@briskteaching.com**.

10. UPDATES TO THIS PRIVACY NOTICE

In short: We may update this Privacy Notice. We will notify you of material changes as described below.
We will update this Privacy Notice from time to time. When we make changes to this Privacy Notice, we will change the “Last Updated” date at the beginning of this Privacy Notice. If we make material changes to this Privacy Notice, we will provide reasonable notice to you, such as by email to your registered email address, by prominent posting on this website or our online services, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided.

As noted above, we will not make any material changes to this Privacy Notice that relate to the collection or use of Student Data without first giving notice to the School and providing a choice before the Student Data are used in a materially different manner than was disclosed when the information was collected.

13. INTERNATIONAL TRANSFERS

13.1 The Standard Contractual Clauses shall, as further set out in Schedule 3, apply to transfers of Covered Data from the Customer to Brisk, and form part of this DPA.

13.2 The Parties agree that execution of the Agreement shall have the same effect as signing the SCCs.

SCHEDULE 1: Details of Processing

A. List of Parties

	Customer	**Customer**
Role	Data exporter (controller)	Data importer (controller / processor)
Contact person	the administrator of the Customer's account as notified to Brisk.	**privacy@briskteaching.com**
Activities relevant to the transfer	The performance of the Agreement.	

B. Description of Processing

Data subjects	**Categories of personal data**	**Sensitive personal data**	**Source of data**	**Nature and purpose of processing**	**Brisk's role in relation to the processing**	**Retention period**
Main points of contact for accounts on the Service held by Educational Institutions ("**Account Administrators**")	**Contact information,** such as name, email address, name of Educational Institution.	None	Collected directly from the data subject.	Communicate with Account Administrators in relation to the administration of the Agreement and relationship between the parties. Send promotional emails in accordance with Account Administrator's preferences. Identify ways in which Brisk can improve the Service and fix errors in the Service.	Controller	For the duration of the Agreement and for 6 years thereafter.
	Account preferences in relation to promotional messages.					Until the relevant Account Administrator is replaced or the Agreement is terminated, and for 2 years thereafter.
	Questions, comments and other correspondence submitted by the Account					2 years, unless any correspondence is identified as relevant to a

	Administrator in relation to the Service.					potential legal claim.
Teachers with accounts on the Service that are associated with, authorized by or paid for by an Educational Institution ("**Teachers on School Accounts**").	**Contact information,** such as name, email address, name of Educational Institution.	None	Collected directly from the data subject or provided by the Educational Institution	Provision of access to the features and functionalities of the Service, including personalization of the Service. Provision of service-related communications in accordance with the data subject's preferences. Provision of technical support in relation to the Service.	Processor on behalf of the relevant Educational Institution.	Until the earlier of: • termination of the Agreement; and • closure of the relevant account on the Service held by the data subject, either at the request of the controller or following 18 months of inactivity.
	Account preferences in relation to service-related messages. **Account tier**, namely whether the Independent Teacher uses a premium or free account on the Service. **Questions, comments and other correspondence** submitted in relation to the Service. **Subjects taught** and **student year groups or grades**. **Content and materials** created through the Service, including the amendments made to content automatically generated through the Service. **Websites** visited in respect of which the Service is activated. **Feedback** in relation to the content generated through the Service. The **features and functionalities** used on the Service.	None, unless contained in content and materials generated through, or prompts or feedback submitted to the Service.	Collected directly from the data subject.			
Teachers on School Accounts	**Contact information,** such as name, email address, name of Educational Institution.	None	Collected directly from the data subject.	Distribution of promotional emails in accordance with the data subject's preferences. Informing product development and improvement.	Controller	For the duration of the Agreement and for 6 years thereafter.
	Account preferences in relation to promotional messages.					Until 2 years after closure of the data subject's account on the Service, either at the

						request of the data subject or following 18 months of inactivity.
	Questions, comments and other correspondence submitted in relation to the Service.					2 years, unless any correspondence is identified as relevant to a potential legal claim.
	The **features and functionalities** used on the Service.					This information is stored in aggregated and anonymized form.
	Subjects taught and **student year groups or grades**.					the administrator of the Customer's account as notified to Brisk.
Teachers on School Accounts	**Device used to access the Service**, such as IP address.	None	Collected directly from the data subject.	Provision of access to the features and functionalities of the Service, including facilitating login and remedying login problems.	Processor on behalf of the relevant Educational Institution.	Up to 90 days.
Teachers with individual accounts on the Service and whose use of the Service is not associated with, authorized by or paid for by an Educational Institution ("**Independent Teachers**")	**Referrals**, namely the number of other Teachers referred by the Independent Teacher to the Service.	None	Collected directly from the data subject.	Manage Brisk's referral program, including managing reward or promotional access to premium features.	Controller	For the duration of the Agreement.
	Professional development courses undertaken and completed through the Service.		Professional development provider partners.	Granting access to premium features linked to the completion of professional development courses.		
Independent Teachers	**Contact information,** such as name, email address, name of Educational Institution.	None, unless contained in content and materials generated through, or prompts or feedback submitted to the Service.	Collected directly from the data subject.	Provision of access to the features and functionalities of the Service, including personalization of the Service. Processing subscription payments. Provision of service-related communications in accordance with the	Controller	For the duration of the Agreement and for 6 years thereafter.
	Account tier, namely whether the Independent Teacher uses a premium or free account on the Service.					For the duration of the Agreement and for 6 years thereafter.
	Payment information, such as credit or debit card					For the duration of the Agreement

	and billing address.			data subject's preferences. Provision of technical support in relation to the Service. Distribution of promotional emails in accordance with the data subject's preferences. Informing product development and improvement.		
	Account preferences in relation to service-related and promotional messages.					For the duration of the Agreement and for 2 years thereafter.
	Questions, comments and other correspondence submitted in relation to the Service.					2 years, unless any correspondence is identified as relevant to a potential legal claim.
	Subjects taught and **student year groups or grades**.					For the duration of the Agreement.
	Content and materials created through the Service, including the amendments made to content automatically generated through the Service.					For the duration of the Agreement.
	Websites visited in respect of which the Service is activated.					For the duration of the Agreement.
	Feedback in relation to the content generated through the Service.					For the duration of the Agreement.
	The **features and functionalities** used on the Service.					This information is stored in aggregated and anonymized form.
	Device used to access the Service, such as IP address.	None		Provision of access to the features and functionalities of the Service, including facilitating login, remedying login problems and load balancing.		Up to 90 days.
Students	**Contact information**, such as name, email address and name of Educational Institution or Teacher granting access.	None	Provided by Customer.	Provision of access to the features and functionalities of the Service, including personalization of the Service.	Processor on behalf of the relevant Educational Institution or Independent Teacher.	Until the earlier of: • termination of the Agreement; and

						• closure of the relevant account on the Service held by the data subject, either at the request of the controller or following 18 months of inactivity.
	Work uploaded and reviewed through the Service. **Interaction with materials generated through the Service**. **Feedback on work uploaded and reviewed** through the Service. **Interaction with educational chatbots** on the Service.	Any sensitive personal data contained in work product or interactions uploaded to the Service by the Student.	Collected directly from the data subject.			the administrator of the Customer's account as notified to Brisk.
	Device used to access the Service, such as IP address.	None		Provision of access to the features and functionalities of the Service, including facilitating login and remedying login problems.		Up to 90 days.
All users	**Device used to access the Service**, such as IP address.	the administrator of the Customer's account as notified to Brisk.	None	Collected directly from the data subject.	Controller	Up to 90 days.

C. Competent Supervisory Authority

The competent supervisory authority is the Irish Data Protection Commissioner.

SCHEDULE 2: Technical and Organizational Measures

Brisk Data Processing Addendum

Effective Date: August 22, 2024

This Data Processing Addendum ("**DPA**") supplements and forms part of the agreement between Brisk Labs Corp. ("**Brisk**") and the Educational Institution or (where applicable) a Teacher in relation to the transfer and processing of Covered Data in connection with the provision of the Service.

1. DEFINITIONS

1.1 Unless otherwise defined in this DPA, capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"**Agreement**" means the agreement entered into between Brisk and the Customer incorporating the terms at **https://www.briskteaching.com/terms** or as otherwise agreed between the parties.

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time, including (without limitation) the GDPR.

"**Authorized Sub-processor**" means the Sub-processors listed in Schedule 4, and any other Sub-processors appointed in accordance with paragraph 7.4.

"**Controller Purposes**" means: (a) undertaking internal research and development to develop, test, improve and alter the functionality of Brisk's products and services; (b) creating anonymized datasets for training or evaluation of Brisk's products and services; and (c) administering Customer accounts on the Service and managing Brisk's relationship with the Customer under the Agreement, in each case as further described in Schedule 1.

"**Covered Data**" means Personal Data that is: (a) provided by or on behalf of the Customer to Brisk in connection with the provision of the Service; or (b) obtained, developed, produced or otherwise Processed by Brisk, or its agents or subcontractors, for the purposes of providing the Service, in each case as further described in Schedule 1.

"**Customer**" means the Educational Institution or a Teacher that enters into the Agreement with Brisk in relation to the Service.

"**Data Subject**" has the meaning given to it in the GDPR.

"**Effective Date**" means the date Brisk and the Customer enter into the Agreement.

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**", as defined in section 3(10) of the Data Protection Act 2018.

"**Personal Data**" has the meaning given to it in the GDPR.

"**Processing**" has the meaning given to it in the GDPR, and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 and available at **https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en**.

"**Sub-processor**" means a processor engaged by another processor to carry out the instructions of the controller.

"**Swiss Data Protection Laws**" means the Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**") and the Swiss Data Protection Ordinance of 31 August 2022 (the "**Ordinance**"), and any new or revised version of these laws that may enter into force for time to time.

1.2 The terms "**controller**" and "**processor**" have the meanings given to them in the GDPR.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA is incorporated into and forms an integral part of the Agreement. This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Covered Data.

3. ROLE OF THE PARTIES

3.1 The Parties acknowledge and agree that:

a. save as set out in paragraph 3.1, Brisk Processes Covered Data as a processor in the performance of its obligations under the Agreement and this DPA and Customer acts as a controller; and

b. Brisk acts as a controller with respect to the Processing of Covered Data for the Controller Purposes as identified in Schedule 1.

4. DETAILS OF DATA PROCESSING

4.1 The details of the Processing of Personal Data under the Agreement and this DPA (including subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in Schedule 1 to this DPA.

4.2 Other than in respect of its Processing of Covered Data for the Controller Purposes:

a. Brisk will only Process Covered Data under the instructions provided by the Customer and in accordance with Applicable Data Protection Laws; and

b. the Agreement and this DPA shall constitute the instructions to Brisk for the Processing of Covered Data by Brisk, and the Customer may issue further written instructions in accordance with this DPA.

4.3 Brisk will:

a. provide the Customer with information to enable the Customer to conduct and document any data protection impact assessments and prior consultations with supervisory authorities required under Applicable Data Protection Laws; and

b. promptly inform the Customer if, in its opinion, an instruction from the Customer infringes Applicable Data Protection Laws.

5. COMPLIANCE

5.1 The Customer shall comply with its obligations under Applicable Data Protection Laws and shall ensure that:

a. any instructions to Brisk in relation to the Processing of Covered Data comply with Applicable Data Protection Laws;

b. it provides such information to Data Subjects regarding the Processing of Covered Data by Brisk as required under Applicable Data Protection Laws;

c. it promptly notifies Brisk of any request received from a Data Subject to exercise their rights under Applicable Data Protection Laws.

6. CONFIDENTIALITY AND DISCLOSURE

6.1 Brisk shall:

a. limit access to Covered Data to personnel who have a business need to have access to such Covered Data; and

b. ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data to which they have access.

7. DEFINITIONS

7.1 Brisk may Process Covered Data anywhere that Brisk or its Sub-processors maintain facilities, subject to the remainder of this paragraph 7 and any restrictions on onward transfers contained in the SCCs.

7.2 The Customer grants Brisk general authorization to engage any Authorized Sub-processor to Process Covered Data.

7.3 Brisk shall:

a. enter into a written agreement with each Authorized Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Brisk's obligations under this DPA; and

b. remain liable for each Authorized Sub-processor's compliance with the obligations under this DPA.

7.4 Brisk will provide the Customer with at least fourteen (14) days' notice of any proposed changes to the Authorized Sub-processors. The Customer shall notify Brisk if it objects to the proposed change to the Authorised Sub-processors (including, where applicable, when exercising its right to object under clause 9(a) of the SCCs) by providing Brisk with written notice of the objection within seven (7) days after Brisk has provided notice to the Customer of such proposed change (an "**Objection**").

7.5 In the event the Customer submits an Objection, Brisk and the Customer shall work together in good faith to find a mutually acceptable resolution to address such Objection. If Brisk and the Customer are unable to reach a mutually acceptable resolution within a reasonable timeframe, which shall not exceed thirty (30) days, Brisk may terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to the Customer.

8. DATA SUBJECT RIGHTS REQUESTS

8.1 Brisk will notify the Customer without undue delay of any request received by Brisk or any Authorised Sub-processor from a Data Subject to assert their rights under Applicable Data Protection Laws in relation to Covered Data Processed by Brisk as a processor or Sub-processor (a "**Data Subject Request**").

8.2 Other than in respect of Brisk's Processing of Covered Data for the Controller Purposes, as between Brisk and the Customer, the Customer will have sole discretion in responding to the Data Subject Request. Brisk shall not respond to the Data Subject Request without the Customer's prior consent, save that Brisk may advise the Data Subject that their request has been forwarded to the Customer.

8.3 Brisk will provide the Customer with reasonable assistance as necessary for the Customer to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests in respect of Covered Data.

9. SECURITY

9.1 Brisk will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Covered Data, including, without limitation, protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage of or to Covered Data.

9.2 When assessing the appropriate level of security, Brisk shall take into account the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

9.3 Brisk will implement and maintain as a minimum standard the measures set out in Schedule 2.

10. INFORMATION AND AUDITS

10.1 The Customer may audit Brisk's compliance with this DPA in respect of its Processing of Covered Data. The Parties agree that all such audits will be conducted:

a. not more than annually, unless more frequent audits are required by a supervisory authority with jurisdiction over the Processing of Covered Data or otherwise under Applicable Data Protection Laws;

b. upon reasonable written notice to Brisk;

c. only during Brisk's normal business hours; and

d. in a manner that does not materially disrupt Brisk's business or operations.

10.2 With respect to any audits conducted in accordance with paragraph 10.3:some text

a. the Customer may engage a third-party auditor to conduct the audit on its behalf, save that Brisk may reasonably object to the engagement of a third-party auditor if such third-party auditor is a competitor of Brisk; and

b. Brisk shall not be required to facilitate any such audit unless and until the Parties have agreed in writing the scope and timing of such audit.

10.3 The Customer shall promptly notify Brisk of any non-compliance discovered during an audit.

10.4 The results of the audit shall be Brisk's confidential information.

10.5 Brisk shall provide to the Customer upon request, or may provide to the Customer in response to any audit request submitted by the Customer to Brisk, either of the following:

a. data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company; or

b. such other documentation reasonably evidencing the implementation of the technical and organizational data security measures in accordance with industry standards.

10.6 If an audit requested by the Customer is addressed in the documents or certification provided by Brisk in accordance with paragraph 10.7, and:

a. the certification or documentation is dated within twelve (12) months of the Customer's audit request; and

b. Brisk confirms that there are no known material changes in the controls audited,

The Customer agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

11. SECURITY INCIDENTS

11.1 Brisk shall notify the Customer in writing without undue delay after becoming aware of any Security Incident.

11.2 Brisk shall take reasonable steps to contain, investigate, and mitigate any Security Incident, and shall send the Customer timely information about the Security Incident, to the extent known to Brisk or as the information becomes available to Brisk,

including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation.

11.3 Brisk shall provide reasonable assistance with the Customer's (or, where applicable, its Customers') investigation of any Security Incidents and any of the Customer's (or, where applicable, its Customers') obligations in relation to the Security Incident under Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

11.4 Brisk's notification of or response to a Security Incident under this paragraph 11 shall not be construed as an acknowledgement by Brisk of any fault or liability with respect to the Security Incident.

12. TERM, DELETION AND RETURN

12.1 This DPA shall commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Brisk's deletion of all Covered Data as described in this DPA.

12.2 Brisk shall:

a. if requested to do so by the Customer (on behalf of its Customers, as appropriate) within thirty (30) days of expiry of the Agreement (the "**Retention Period**"), provide a copy of all Covered Data in such commonly used format as requested by the Customer, or provide a self-service functionality allowing the Customer to download such Covered Data; and

b. on expiry of the Retention Period, delete all copies of Covered Data Processed by Brisk or any Authorised Sub-processors, other than any Covered Data that Brisk is required to retain to comply with applicable law, to pursue or defend legal claims or for the Controller Purposes.

Brisk assigns personnel with responsibility for the determination, review and implementation of security policies and measures.

Brisk:

- has documented the security measures it has implemented in a security policy and/or other relevant guidelines and documents;
- reviews its security measures and policies on a regular basis to ensure they continue to be appropriate for the data being protected.

Brisk establishes and follows secure configurations for systems and software and ensures that security measures are considered during project initiation and the development of new IT systems.

Breach response

Brisk has a breach response plan that has been developed to address data breach events. The plan is regularly tested and updated.

Intrusion, anti-virus and anti-malware defenses

Brisk's IT systems used to process personal data have appropriate data security software installed on them, including industry standard firewall, anti-virus, anti-malware and intrusion detection systems.

Brisk collects, maintains and reviews event logs to identify suspicious activity.

Access controls

Brisk limits access to personal data by implementing appropriate access controls, including:

- limiting administrative access privileges and use of administrative accounts;
- changing all default passwords before deploying operating systems, assets or applications;
- requiring authentication and authorization to gain access to IT systems (i.e. requiring users to enter a user id and password before they are permitted access to IT systems);
- measures to ensure least privilege access to IT systems;
- appropriate procedures for controlling the allocation and revocation of personal data access rights. For example, having in place appropriate procedures for revoking employee access to IT systems when they leave their job or change role;
- use of multi-factor authentication to access data on Brisk's systems;

- automatic timeout and locking of user terminals if left idle;
- access to IT system is blocked after multiple failed attempts to enter correct authentication and/or authorization details;
- monitoring and logging access to IT systems;
- monitoring and logging amendments to data or files on IT systems.

Availability and Back-up personal data

Brisk has a documented disaster recovery plan that ensures that key systems and data can be restored in a timely manner in the event of a physical or technical incident. The plan is regularly tested and updated.

Brisk regularly backs-up information on IT systems and keeps back-ups in separate locations. Back-ups of information are tested regularly.

Segmentation of personal data

Brisk:

- separates and limits access between network components and, where appropriate, implements measures to provide for separate processing (storage, amendment, deletion, transmission) of personal data collected and used for different purposes;
- does not use live data for testing its systems.

Disposal of IT equipment

Brisk:

- has in place processes to securely remove all personal data before disposing of IT systems;
- uses appropriate technology to purge equipment of data.

Encryption

Brisk encrypts data at rest using AES-256 and in transit using TLS 1.2 or higher.

Encryption keys are stored separately from the encrypted information.

Transmission or transport of personal data

Appropriate controls are implemented by Brisk to secure personal data during transmission or transit, including:

- encryption in transit;
- logging personal data when transmitted electronically.

Device hardening

Brisk ensures that all virtual machines are hardened in accordance with the Center for Internet Security (CIS) Benchmarks.

Asset and Software management

Brisk maintains an inventory of IT assets and the data stored on them, together with a list of owners of the relevant IT assets.

Brisk:

- documents and implements rules for acceptable use of IT assets.
- requires network level authentication and uses client certificates to validate and authenticate systems;
- deploys automated patch management tools and software update tools for operating systems and software;
- proactively monitors software vulnerabilities and promptly implements any out of cycle patches;
- permits the use of only the latest versions of fully supported web browsers and email clients.

Brisk stores all API keys securely, including as follows:

- Brisk stores API keys directly in its environment variables;
- Brisk does not store API keys on client side;
- Brisk does not publish API key credentials in online code repositories (whether private or not); and
- Brisk uses API key management tools to retrieve and manage credentials for large development projects.

Staff training and awareness

Brisk's agreements with staff and contractors and employee handbooks set out its personnel's responsibilities in relation to information security.

Brisk carries out:

- regular staff training on data security and privacy issues relevant to their job role and ensures that new starters receive appropriate training before they start their role (as part of the on boarding procedures);
- appropriate screening and background checks on individuals that have access to sensitive personal data.

Brisk ensures that information security responsibilities that are applicable immediately before termination or change of employment and those which apply after termination / change of employment are communicated and implemented.

Staff are subject to disciplinary measures for breaches of Brisk's policies and procedures relating to data privacy and security.

Selection of service providers and commission of services

Brisk assesses service providers' ability to meet their security requirements before engaging them.

Brisk has written contracts in place with service providers which require them to implement appropriate security measures to protect the personal data they have access to and limit the use of personal data in accordance with Brisk's instructions.

Part 2

Assistance with Data Subject Rights Requests

Brisk has implemented appropriate policies and measures to identify and address data subject rights requests, including:

- Brisk maintains accurate records to enable it to identify quickly all personal data processed on behalf of the Customer; and
- back-ups of personal data processed by Brisk on behalf of the Customer are overwritten on a regular basis and in any event every thirty (30) days to ensure deletion and rectification requests are fully actioned.

SCHEDULE 3: STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

With respect to any transfers referred to in clause 13, the Standard Contractual Clauses shall be completed as follows:

1.1 Module Two (*controller to processor*), or as appropriate, Module Three (*processor to processor*) of the SCCs will apply to Brisk's Processing of Covered Data.

1.2 Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

1.3 Option 2 of Clause 9(a) (*General written authorization*) shall apply, and the time period to be specified is determined in clause 7.4 of the DPA.

1.4 The option in Clause 11(a) of the Standard Contractual Clauses *(Independent dispute resolution body*) does not apply.

1.5 With regard to Clause 17 of the Standard Contractual Clauses (*Governing law*), the Parties agree that option 1 will apply and the governing law will be Irish law.

1.6 In Clause 18 of the Standard Contractual Clauses (*Choice of forum and jurisdiction*), the Parties submit themselves to the jurisdiction of the courts of Ireland.

1.7 For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.

1.8 For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organizational measures.

2. UK Addendum

2.1 This paragraph 2 (*UK Addendum*) shall apply to any transfer of Covered Data from the Customer (as data exporter) to Brisk (as data importer), to the extent that:

a. the UK Data Protection Laws apply to the Customer when making that transfer; or

b. the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid

before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:some text

a. the "Addendum EU SCCs" shall refer to the SCCs as they are incorporated into this Agreement in accordance with clause 13 and this Schedule 3;

b. Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

c. the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

d. for the purposes of Table 4 of the Approved Addendum, Brisk (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum; and

e. Section 16 of the Approved Addendum does not apply.

3. Swiss addendum

3.1 This Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws.

3.2 **Interpretation of this Addendum**

a. Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"**Addendum**" means this addendum to the Clauses;
"**Clauses**" means the Standard Contractual Clauses as incorporated into this DPA in accordance with paragraph 13 and as further specified in this Schedule 3; and
"**FDPIC**" means the Federal Data Protection and Information Commissioner.

b. This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfils the Parties' obligations under Article 16(2)(d) of the FADP.

c. This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

d. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

e. In relation to any Processing of Personal Data subject to Swiss Data Protection Laws, this Addendum amends and supplements the Clauses to the extent necessary so they operate:some text
    a. for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter’s Processing when making that transfer; and

    b. as standard data protection clauses approved, issued or recognised by the FDPIC for the purposes of Article 16(2)(d) of the FADP.

3.3 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 Changes to the Clauses

a. To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.3(a)) the following amendments are made to the Clauses:
    a. References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

    b. Clause 6 Description of the transfer(s) is replaced with:

    c. "The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter’s Processing when making that transfer."

d. References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

e. References to Regulation (EU) 2018/1725 are removed.

f. References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

g. Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

h. Clause 17 is replaced to state: "These Clauses are governed by the laws of Switzerland".

i. Clause 18 is replaced to state: "Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

SCHEDULE 4: Authorised Sub-Processors

Sub-processor	**Description**
Datadog Inc	Site Reliability and monitoring tool that helps track performance, detect issues, and improve user experience through real-time data insights and visualizations
Amazon.com, Inc	Hosts databases and servers that power and backup Brisk
Snowflake Inc.	Serves as a data warehouse that powers Brisk
Mode Analytics, Inc.	Runs various data reports on data previously captured in Snowflake so we can improve the tool.
Google LLC (Alphabet Inc.)	Provides single-sign-on (SSO) authentication for Brisk users, hosts student coursework and teacher-generated content.
Segment (Twilio Inc.)	Logging and analytics tool that helps developers understand how users interact with Brisk
OpenAI, Inc.	Artificial Intelligence Services
Anthropic running on AWS Bedrock	Artificial Intelligence Services
Sentry (Functional Software, Inc.)	Site Reliability and monitoring tool that helps developers identify, diagnose, and fix issues and

	improve the user experience
GPTZero Inc.	Text Analysis tool that helps detect AI-generated text
Sapling	Text Analysis tool that helps improve writing by providing grammar and style suggestions
Salesforce	Houses and tracks partnership agreements, points of contact and other coordination information.
Zendesk	Customer service platform that manages support, tickets, and customer interactions
Microsoft Azure	Hosts databases and servers that power and backup Brisk
Klaviyo	Cloud-based email tool
MixPanel	Logging and analytics tool that helps developers understand how users interact with Brisk
Posthog	Analytics tool that tracks user behavior and helps improve product development and user experience
Ednition	A secure integration tool that enables secure data syncing from any SIS or other third party rostering tool into Brisk
Classlink	A single sign-on and rostering platform used by districts to manage secure access to educational tools
Clever	A platform that enables secure, automated rostering and SSO for K–12 schools
Perplexity	AI-powered search tool that helps Brisk answer user questions by retrieving and citing information from public sources.