DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is dated __11th of October 2023__ and is between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools ("District") and [Tutteo Inc.] ("Contractor"). This Addendum applies to all services provided by Contractor to District through the Contract, as defined herein. The Addendum and the Contract are collectively referred to hereinafter as "Agreement". This Addendum is hereby incorporated into the Contract. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect.

In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. "*Act*" means the Colorado Student Data Transparency and Security Act, C.R.S. § 22-16-101 et seq., as amended from time to time.

1.2. "*Biometric Record*," as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.3. "*Click-Wrap*" means both the act of accepting on-line terms and conditions of a Vendor Agreement without ink or paper, by clicking on an on-line button or link for that purpose, and the resulting agreement.

1.4. "*Contract*" means the contract, service order, purchase order, invoice, or any other form of agreement that may now or in the future exist between Contractor and District, specifically including [Flat for Education] dated __11/10/2023___.

1.5. "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.6. "*District Data*" means:

1.6.1. Any and all PII, Record, and Education Records; and

1.6.2. Any and all PII included therein or derived therefrom; and

1.6.3. Health, medical, financial, contract, and employment information about students, employees, and contractors, and their respective families that is protected by various State and federal laws applicable to the Contract or the Addendum or both;

1.6.4. All data and metadata about Data and PII that the Contractor collects, generates, or infers; and

1.6.5. All data and metadata that students generate or infer by using the Services that collect the data; and

1.6.6. Data and information that the District makes available directly or indirectly to the Contractor; and

1.6.7. Data and information that the District DOES NOT also intentionally make or HAS NOT intentionally made generally available on public websites or publications.

1.7. "*De-identified Data*" means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.8. "*Education Records*" means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.9. "*End User*" means individuals authorized by the District to access and use the Services as defined herein.

1.10. "*Incident*" means an adverse event that may affect the confidentiality, integrity or availability of data, or an event that is a violation of security or privacy policies.

1.11. "*Mine*" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.12. "*Personally Identifiable Information*" or "*PII*" means information and metadata that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by the District, either directly or through the Services, or by Contractor. PII also includes other information that, alone or in combination, is linked or or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates. Personally Identifiable Information includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 et seq. ("CORA"); (b) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (c) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (e) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; and (f) other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

1.13. "*Record*" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.14. "*Securely Destroy*" means to remove District Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") Special Publication 800-88 Guidelines for Media Sanitation (December 2014), or such other standard to which the District's Chief Privacy Officer or designee may agree in writing, so that District Data is permanently irretrievable in Contractor's and Subcontractors' normal course of business.

1.15. "*Security Breach*" means an incident where sensitive, protected, or confidential data is altered, copied, transmitted, viewed, stolen, or used by an unauthorized party, or released to an untrusted environment.

1.16. "*Services*" means what that term is defined in the Contract, and also includes any goods or services acquired by the District from the Contractor, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet, installed or run on a computer or electronic device.

1.17. "*Subcontractor*" means Contractor's subcontractors, agents, or any other third party identified on Schedule 2, as updated by Contractor from time to time in accordance with the requirements of this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.18. "*Student Profile*" means a collection of PII data elements relating to a student of the District.

1.19. *"Targeted Advertising"* means selecting and sending advertisements to individuals based on information obtained or inferred over time from the individual's online behavior, use of applications, or PII; but if the Contractor is also a School Service Contract Provider or otherwise subject to compliance with the Act , then the Act definition of that term, if different from this definition, governs.

1.20. "*Vendor Agreement*" means any form of agreement or documentation provided by the Contractor, including without limitation, an on-line agreement, proposal, or invoice, whether made a part of the Agreement or effective or purporting to be effective outside of the Agreement.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, including without limitation, De-identified Data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its obligations specified in the Contract. This Addendum does not give Contractor any rights, title, or interest, including all intellectual property and proprietary rights, implied or otherwise,to District Data or De-identified Data.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, Mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2 Use District Data for its own commercial benefit, including but not limited to, Targeted Advertising or any advertising, marketing, or surveying of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Addendum or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor's privacy policy;

3.2.4 Use District Data to create a Student Profile other than as authorized or required by the Contract to perform the Services; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties under the Contract for District's and its End Users' benefit and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as required by law, or if authorized in writing by the District. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Addendum, it has not been found in violation of FERPA by the U.S. Department of Education's Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract;

(d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; (e) Subcontractor shall indemnify the District in accordance with the terms set forth in Section 10 of this Addendum; and (f) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees and Subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Addendum. Contractor shall also ensure that its Subcontractors comply with the insurance requirements specified in Section 11 of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. As required by § 22-16-108(2) of the Act, prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

3.7 Misuse/Unauthorized Release. Upon discovering the misuse or unauthorized release of Personally Identifiable Information held in connection with this Addendum by Contractor, a Subcontractor or a subsequent Subcontractor of Contractor, Contractor will notify the District as soon as possible, regardless of whether the misuse or unauthorized release is a result of a material breach of the terms of this Addendum.

4. Data Security

4.1 Security Safeguards. Contractor shall maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of District Data. Contractor shall store and process District Data in accordance with industry standards and best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in CIS Critical Security Controls (CIS Controls), as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, including without limitation the Act, as well as the terms and conditions of this Addendum. Without limiting

the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended, or such other standard as the District's Chief Privacy Officer or designee may agree to in writing. Contractor shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Contractor shall fully encrypt disks and storage for all laptops and mobile devices.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including without limitation audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is deidentified in accordance with this Addendum.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, one or more of the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) a third-party network security audit report; (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred; (3) District Data has been deidentified by Contractor as set forth in the definition of Deidentified Data in section 1.7 of this Addendum.

4.5 Background Checks.

4.5.1 If Contractor has access to District Data, but does not provide direct services to students, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check per Contractor's internal employment policies. "Direct services to students" includes, but is not limited to: instruction; physical, mental, and social health supports; transportation; and food services, which are provided to students at least one time per month during the school year.

4.5.2 If Contractor provides direct services to students and has access to student data, the Contractor and every person, including any subcontractor or agent of the Contractor, shall be required to have a criminal background check that meets the requirements of § 22-32-109.7, C.R.S. and other District requirements, including a fingerprint-based conviction investigation. Conducting a Colorado Bureau of Investigation criminal history check or a Name Check investigation for any person providing services under this Contract does not meet District requirements. The costs associated with the background checks are solely the Contractor's responsibility. Thereafter, any personnel, subcontractor, volunteer or agent hired or added during the term of this Contract shall satisfy the requirements set forth in this Section before performing services on Contractor's behalf. The Contractor shall make the background check results available

upon request of the District in compliance with the provisions of § 24-72-305.3, C.R.S. The District also reserves the right to conduct its own criminal background check of every person before Services begin.

4.5.3 Notwithstanding the criminal background check requirement as set forth above, Contractor hereby certifies that no employee, subcontractor, volunteer or agent of the Contractor performing the Services has been convicted in Colorado or in any other State of a criminal offense involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence. Contractor shall notify the District immediately upon the discovery or receipt of any information that any person performing services on Contractor's behalf has been detained or arrested by a law enforcement agency of the aforementioned crimes. Contractor understands that allowing any employee, subcontractor, volunteer or agent of the Contractor performing the Services who has been arrested or convicted of the aforementioned crimes to: (i) provide direct services to students, (ii) access student data, or (iii) enter onto District property, constitutes a material breach of this Contract and may result in the immediate termination of this Contract and referral to law enforcement for possible criminal charges, or additional civil sanctions pursuant to federal and state law. Misdemeanor conviction(s) may not necessarily result in the immediate termination of this Contract. Misdemeanor convictions are evaluated on a case-by-case basis, considering the nature and gravity of the offense, time elapsed since the offense, conviction, or time served, and the nature of the Services. Upon the District's request, Contractor shall provide documentation of every person performing the Services to substantiate the basis for this certification.

4.5.4 The Contractor and every person, including any subcontractor or agent of the Contractor, performing the Services, or who is on District's property, may be scanned through the Visitor Management System. If an individual's identity cannot be verified through an acceptable form of identification (driver's license or state ID), they will not be allowed on District's property.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. Immediately upon becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as

otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within seven (7) calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require Contractor to amend its remediation plans.

5.4 Effect of Security Breach. Upon the occurrence of a Security Breach, the District may terminate this Agreement in accordance with District policies. The District may require Contractor to suspend all Services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which Services were not rendered. Contractor acknowledges that, as a result of a Security Breach, the District may also elect to disqualify Contractor and any of its Subcontractors from future contracts with the District.

5.5 Liability for Security Breach. In addition to any other remedies available to the District under law, contract, or equity, Contractor shall reimburse the District in full for all costs, including but not limited to, payment of legal fees, audit costs, fines, and other fees imposed that were actually incurred by the District and caused in whole or in part by Contractor or by Contractor's Subcontractors for any Security Breach. If required by law or contract, Contractor shall provide notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities. Contractor shall provide one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during any Security Breach could be used to commit financial identity theft.

6. Response to Legal Orders, Demands or Requests for Data

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, including but not limited to, a request pursuant to the CORA, the District will promptly notify Contractor and, within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA or the Act, the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor shall promptly notify the District and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4 Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

7. Compliance with Applicable Law

7.1. School Service Contract Providers. If Contractor provides a "school service", which is defined as an Internet website, online service, online application or mobile application that: (a) is designed and marketed primarily for use in a preschool, elementary school or secondary school; (b) is used at the direction of District teachers or other District employees; and (c) collects, maintains or uses District Data or PII, then Contractor is a "school service contract provider" under the Act. If that is the case, Contractor must complete Schedule 5. Contractor shall update Schedule 5 as necessary to maintain accuracy. District reserves the right to terminate the Contract, or the DPA, or both, as specified in Section 8, should the District receive information after the Effective Date that significantly modifies Contractor's representations made in this Section 7.1.

7.2 Children's Online Privacy and Protection Act. If Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations ("COPPA")) from children under thirteen (13) years of age in performing the Services, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with written notice of its collection, use, and disclosure practices.

7.3 Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the Services including but not limited to: (a) COPPA; (b) FERPA; (c) the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) the Health Information Technology for Economic and Clinical Health Act, (e) Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (f) Payment Card Industry Data Security Standards; (g) Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; and (h) Americans with Disabilities Act, and Federal Export Administration Regulations.

7.4 Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will require that its system and services will, at a minimum, conform with all laws, regulations and guidance that apply to accessibility in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973, and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and services provided or developed by the District including District content.

8. Termination of the Contract

8.1 The District may immediately terminate the Contract in accordance with District policies if, at any time, the District determines in its sole discretion, that Contractor has breached any of the requirements of this Addendum. Should Contractor not comply with the requirements of this Addendum and that non-compliance results in the misuse or unauthorized release of PII by the Contractor, the District may terminate the Contract immediately as provided under this Addendum and in accordance with C.R.S. Section 22-16-107 (2)(a).

8.2. The District may terminate the Contract if the District receives information after execution of this Addendum, that any of Contractor's representations or warranties have substantially changed after execution of this Addendum, including but not limited to the terms of Contractor's privacy policy.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Addendum, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than (30) calendar days after termination or expiration of this Addendum, Contractor shall certify in writing that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data or Contract Data that is in Contractor's possession or in the possession of Contractor's Subcontractors transferred to a third party designated by the District, such transfer shall occur within a reasonable period of time but no later than thirty (30) calendar days after expiration or termination of this Agreement, and without significant interruption in service or access to such District Data. Contractor shall work closely with such third party transferee to ensure that such transfer/migration uses facilities and methods compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. District will pay all costs associated with such transfer, unless such transfer is as the result of termination of this Agreement following Contractor's breach of the terms of this Agreement. Upon successful transfer of District Data, as confirmed in writing by the District's Designated Representative, Contractor shall Securely Destroy all District Data in accordance with Section 9.1.

9.3 Response to Specific Data Destruction or Return Requests. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District.

10. Indemnification

10.1 If Contractor is a "public entity" then it will be responsible for the negligent acts and omissions of its officers, agents, employees and representatives with respect to its obligations under this Agreement. Any provision of this Agreement, whether or not incorporated herein by reference, shall be controlled, limited and otherwise modified so as to limit any liability of the Contractor under the Colorado Governmental Immunity Act, C.R.S. 24-10-101 et seq. It is specifically understood and agreed that nothing contained in this paragraph or elsewhere in this Agreement shall be construed as an express or implied waiver of its governmental immunity or as an express or implied acceptance of liabilities arising as a result of actions which lie in tort or could lie in tort in excess of the liabilities allowable under the Act, as a pledge of the full faith and credit of the Partner, or as the assumption by the Partner of a debt, contract or liability of the District or its affiliates in violation of Article Xl, Section 1 of the Constitution of the State of Colorado.

10.2 If Contractor is not a "public entity" then Contractor shall indemnify, defend and hold District and its elected officials, employees, representatives, and agents harmless, without limitation, from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses, including attorneys' fees, the costs of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from Contractor's, or Contractor's subcontractors, performance of services under this Addendum, any third-party claim against any Indemnified party

to the extent arising out of or resulting from Contractor's, or Contractor's subcontractors, failure to comply with any of its obligations under Sections 3, 4, 5, and 9 of this Addendum, and any breach of Contractor's, or Contractor's subcontractors, obligations under this Addendum. These indemnification duties shall survive termination or expiration of this Agreement.

11. Insurance

11.1 Coverage. As required by Schedule 6.

12. EULAs, Terms of Use, and other License Agreements

12.1 The Contractor grants such licenses and user permissions and provides the Services under those conditions as set forth in Schedule 7 attached hereto.

12.2 Click-Wrap and Exclusions. If Schedule 7 is blank or not attached, the Contractor grants such licenses and user permissions as the District may accept by Click-Wrap, whether with the Contractor or provided through a Subcontractor. Notwithstanding any such Click-Wrap terms and conditions, and notwithstanding the provisions in the Agreement or Vendor Agreement, the District DOES NOT agree to any of the following:

12.2.1 Jurisdiction, venue and governing law other than Colorado.
12.2.2 Indemnification by the District of any person.
12.2.3 Binding arbitration or any other binding extra-judicial dispute resolution process.
12.2.4 Limitation of Contractor's liability for (i) direct damages; (ii) bodily injury, death or damage to tangible property or (iii) amounts that are less than the insurance coverage the Contractor provides.
12.2.5 Ownership or use of District Data other than as described in this Addendum.
12.2.6 Confidentiality provisions in conflict with the District's obligations under the Colorado Open Records Act and other applicable open records laws.
12.2.7 Fees, penalties, and payment obligations other than as agreed to in the Agreement.

12.3 End Users. In the event that the Contractor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users or with the District ("EULAs"), the parties agree that the terms of this Addendum shall superseded the EULAs.

12.4 Subcontractor Click-Wrap. If the Contractor is providing software or on-line services through Subcontractors, and Click-Wrap will be required for the District to avail itself of the Services under this Agreement, then the Contractor shall cause the Subcontractor providing

such software or on-line access to consent to and honor the terms of this Addendum with respect to the District's use of the Services provided through the Subcontractor.

13. Miscellaneous

13.1 Public Inspection of Agreement. Contractor acknowledges and agrees that this Agreement and all documents Contractor provides District as required herein, are public records for purposes of the CORA and shall at all times be subject to public inspection. The parties understand that in the event of a request for disclosure of such information, the District will notify Contractor to give Contractor the opportunity to redact its proprietary or confidential material. In the event of the filing of a lawsuit to compel disclosure, the District will tender Contractor's material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure or waive the same.

13.2 Survival. The Contractor's obligations under this Addendum, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

13.3 Choice of Law. Any claim, controversy or dispute arising under or related to this Addendum shall be construed pursuant to the substantive, not conflicts, laws of the State of Colorado. Each of the parties submits to the exclusive jurisdiction of any state court sitting in or federal court with jurisdiction over Denver County, Colorado, in any action or proceeding arising out of or relating to this Agreement and agrees that all claims in respect of the action or proceeding may be heard and determined in any such court. Each party also agrees not to bring any action or proceeding arising out of or relating to this Addendum in any other court. Each of the parties waives any defense of inconvenient forum to the maintenance of any action or proceeding so brought and waives any bond, surety or other security that might be required of any other party with respect to any such action or proceeding.

13.4 Immunities. The District retains all of its rights, privileges and immunities under the Colorado Governmental Immunity Act, C.R.S. § 24-10-101 *et seq*.

13.5 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of the District. Any assignment in violation of this section shall be void.

13.6 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

13.7 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 – Designated Representatives
Schedule 2 – Subcontractors
Schedule 3 – Written Consent to Maintain De-identified Data
Schedule 4 – Certification of Destruction\Return of District Data
Schedule 5 – Data Elements
Schedule 6 – Insurance
Schedule 7 – EULAs and Terms of Use

13.8 Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

13.9 Electronic Signatures and Electronic Records. Each party consents to the use of electronic signatures by the other party. This Addendum, and any other documents requiring a signature under this Addendum, may be signed electronically by each party in the manner specified by the District. The parties agree not to deny the legal effect or enforceability of this Addendum solely because it is in electronic form or because an electronic record was used in its formation. The parties agree not to object to the admissibility of the Addendum in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

The parties are signing this Addendum on the date stated in the introductory clause.

“CONTRACTOR”

By: _____ _____
Signature

_____Pierre Rannou_____
Printed name and title

“SCHOOL DISTRICT NO. 1”

APPROVED:

By : _____
Staci Crum
Director, Financial Operations

OPTION 1

SCHEDULE 1
Designated Representatives

NOTICE REQUIRED	DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Security Breach:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: Jim_Lucchesi@dpsk12.org**and **robert_losinski@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
FERPA Records Requests:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org** **Records Requests: https://denverco.scriborder.com/**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
CORA Requests:	**Stacy Wheeler** **CORA Officer** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: cora@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Updates to Privacy Policy / Transparency Requirements:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Updates to Subcontractor Schedule:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Data Retrieval:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: Jim_Lucchesi@dpsk12.org**and **robert_losinski@dpsk12.org**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**
Destruction of Data:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203**	**[TITLE]** **By U.S. Mail: _____** **_____** **By E-mail: _____**

	By E-mail: Jim_Lucchesi@dpsk12.organd **robert_losinski@dpsk12.org**	

OPTION 2

SCHEDULE 1
Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: **Jennifer Collins** **Title:** **Chief Privacy Officer, Deputy General Counsel** **Address:** **1860 Lincoln St** **Denver, CO 80203** **Phone:** **720-423-2211** **E-mail:** **legal_contracts@dpsk12.org**	**Name: Pierre Rannou** **Title: CEO** **Address: 2093 Philadelphia Pike #3615N Claymont, DE, 19703** **Phone: +1 (845) 201 7782** **E-mail: EDU@flat.io**

SCHEDULE 2
Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

What third party vendors does Contractor do business with that may have access to student personally identifiable data, and what is the purpose of these third party vendors (please fill complete the table below with this information)?

https://flat.io/help/en/general/data-infrastructure.html#subprocessors

Name of Subcontractor	Primary Contact Person	Subcontractor's Address	Subcontractor's Phone/email	Purpose of re-disclosure to Subcontractor

SCHEDULE 3
Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	Purpose for Retention and Use	Period of Use

I\We, _____Pierre Rannou_____, as [title] ___CEO_____ and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Name: _____Tutteo inc_____

Contractor Representative Name: _____Pierre Rannou_____

Title: CEO

Signature: _____ Date: 10/11/2023

SCHEDULE 4
Certification of Destruction\Return of District Data

I\We, Pierre Rannou as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on _____, 20___ by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subcontractor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on _____, 20___ to _____, by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subcontractor	*Date of Return*	*Return / Transfer Method*

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 5
Data Elements

(Mandatory to be completed if Contractor is a School Service Contract Provider under CRS 22-16-101 et seq.)

1. **Contractor collects, generates or uses pursuant to the Agreement the following data elements of District Data or PII**:

   IP address, Meta data on user interactions, Language information (preferences), student school enrollment, teacher names, student email address, Vendor/APP assigned student ID Number, Student app Username, Student App password, Student first & Last name, Student generated Content,

2. **Contractor collects and uses the District Data for the following educational purposes**:

Music Theory Education and Band / Choirs conducting

3. **Contractor's policies regarding retention and disposal of District Data are as follows**:

   We remove the data as soon as the agreement is terminated by one of the party.

4. **Contractor uses, shares or discloses the District Data in the following manner:**

   We don't disclose nor shares the District Data. We only use to solely provide the service.

5. **Has Contractor's agreement has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth in this Agreement**?

   ☐ Yes x No.

   If yes, describe:

SCHEDULE 6
Insurance

Contractor agrees to secure, at or before the time of execution of this Agreement, this insurance covering all operations, goods or services provided pursuant to this Agreement.

SCHEDULE 7
EULAs and Terms of Use

Flat for Education DPA

Final Audit Report 2023-10-12

Created:	2023-10-12
By:	Melissa Haran (melissa_haran@dpsk12.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAX00274Uvk4mOfL2W6wE6pdJxUdaWUABq

"Flat for Education DPA" History

Document created by Melissa Haran (melissa_haran@dpsk12.org)
2023-10-12 - 4:11:44 PM GMT

Document emailed to Staci Crum (staci_crum@dpsk12.org) for signature
2023-10-12 - 4:12:15 PM GMT

Email viewed by Staci Crum (staci_crum@dpsk12.org)
2023-10-12 - 4:29:37 PM GMT

Document e-signed by Staci Crum (staci_crum@dpsk12.org)
Signature Date: 2023-10-12 - 4:30:11 PM GMT - Time Source: server

Agreement completed.
2023-10-12 - 4:30:11 PM GMT