UNIVERSITY OF MONTANA
www.umt.edu

MEMORANDUM of UNDERSTANDING:

This Memorandum of Understanding ("MOU") replaces and supersedes the MOU entered into by the parties on January 13, 2026.

Exhibit A

Data Governance Addendum for District Data of the Browning School District #9

Data Governance Conditions. Terms used herein shall have the same meaning as in the Agreement unless otherwise specifically provided. To the extent that Sprigeo ("Company") is permitted, under the applicable terms of the Agreement, to subcontract or otherwise delegate its duties and obligations under the Agreement, Company is likewise permitted to subcontract or delegate the performance of corresponding duties and obligations contained in this exhibit, provided however that Company will remain ultimately responsible for such duties and obligations. To the extent that any provision of this addendum conflict with or contradict the Contract, Terms of Service or Privacy Policy, in letter or spirit, the provisions of the Contract, Terms of Service or Privacy Policy shall prevail.

- **Data Storage/ Maintenance.** The parties agree that all data collected or held by Company (including but not limited to **Browning School District #9** ("Customer") school staff and students' names and other information) shall be stored within the United States of America. The parties further agree that Company shall maintain all data in a secure manner using appropriate technical, physical, and administrative safeguards to protect said data. No data may be backed up outside of the Continental United States.

- **Data Encryption.** In conducting data transactions and transfers with the Customer, Company will ensure that all such transaction and transfers are encrypted.

- **Data Portals.** Company warrants and represents that all of its data portals are secured through the use of verified digital certificates.

- **Data Breach.** Company agrees that it will implement commercially reasonable administrative, physical and technical safeguards designed to secure User Data from Customer from unauthorized access, disclosure, or use, which may include, where commercially reasonable or to the extent required by Law, data encryption, firewalls, and physical access controls to buildings and files. In the event Company has a reasonable, good faith belief that an unauthorized party has accessed or had disclosed to it User Data that the Customer provided Company or that Company collected from Customer or its authorized users, and such access or disclosure occurs in a manner that compromises the security of said User Data ("Security Incident"), then Company will promptly, subject to applicable confidentiality obligations and any applicable law enforcement investigation, or if required by Law in such other time required by such Law,

notify the Customer and will use reasonable efforts to cooperate with the Customer's investigation of the Security Incident.

- If, due to a Security Incident which is caused by the acts or omissions of Company or its agents, employees, or contractors, any third-party notification of such real or potential data breach is required under law, Company shall be responsible for the timing, content, and costs of such legally-required notifications. With respect to any Security Incident which is not due to the acts or omissions of Company or its agents, employees, or contractors, Company shall nevertheless reasonably cooperate in the Customer's investigation and third-party notifications, if any, at the Customer's direction and expense.

  Company shall also be responsible for the cost of investigating any Security Incident determined to be caused by the acts or omissions of Company or its agents, employs, or contractors, as well as the payment of actual, documented costs including reasonable legal fees, audit costs, fines, and other fees imposed against the Customer the steps and processes that Company will take to prevent post-employment data breaches by Company employees after their employment with Company has been terminated.

- **Data Inventory.** Company will provide the Customer with a data inventory that inventories all data fields and delineates which fields are encrypted within Company's platform maintaining collected are encrypted within Company's platform maintaining collected Customer data.

- **Data Ownership.** The parties agree that, notwithstanding Company's possession of or control over Customer data, the Customer maintains ownership of all data that the Customer provides to Company or that Company collects from the Customer. Company further agrees that customer data cannot be used by company for marketing, advertising, or data mining, or shared with any third parties unless allowed by law and expressly authorized by the Customer in writing.

- **Company Access to Customer Data.** The parties agree that Company shall exclusively limit its employees, contractors, and agents' access to and use of Customer data to those individuals who have a legitimate need to access Customer data in order to provide required support of the system or services to the Customer under the Agreement. Company warrants that all of its employees, contractors or agents who have such access to confidential District data will be properly vetted to ensure that such individuals have no significant criminal history.

- **Data Handling in the Event of Termination.** In the event that the parties terminated their agreement for the provisions of Company's services, upon written request any Customer data within Company's possession or control must be provided to the Customer and all other copies of the data must be de-identified/deleted. De-identified data will have all direct and indirect personal identifiers removed, including but not limited to names, addresses, dates of birth, social security numbers, family information, and health information. Furthermore, Company agrees not to attempt to re-identify de-identified data and not transfer de-identified data to any party unless that party agrees not to attempt re-identification. If Customer data is disclosed without de-identifying the same as required herein, written notice shall be provided to the Customer. If Customer data is restored from a back-up after the parties' termination of their agreement for

Company's services, then that data must also be de-identified/deleted.

- **Cyber Security Insurance.** Company will provide to the Customer a certificate of insurance including Cyber Security Insurance coverage for Customer coverage in the event of a Data Breach.

- **Company Visits to Customer Property.** The parties recognize that certain Company employs, contractors, or agents may visit the Customer's property in order to obtain the necessary information for the provision of Company's services. In the even that a Company employee must be unsupervised on Customer's property, the parties agree that, before any such visits to the Customer occur, all visiting Company employees, contractors, or agents must clear both criminal and child abuse & neglect background checks. Company further warrants and agrees that its employees, contractors, or agents who visit the Customer will not have contact or interact with the Customer's students. Company will indemnify, defend, and hold the Customer, its board members, administrators, employees and agents harmless from and against liability for any and all claims, actions, proceedings, demands, costs, (including reasonable attorneys' fees), damages, and liabilities resulting directly, from the acts and/or omissions of Company and/ or its employees, contractors, or agents, subcontractors in connection with visits to the Customer's property as described herein.

EXHIBIT B

- **Purpose and Rules.** Rules adopted herein prescribe the policies and procedures for operation and use of the School Safety Tip Line Program (SSTL). The SSTL is established to facilitate the safety and health of students.

- **Definitions.**

(1) "Anonymous" means not identified by name.

(2) "Confidential Information" means any personally identifiable information acquired by the SSTL, its staff, schools, school districts, Education Service Districts, service providers and local law enforcement, or information that is confidential under other state or federal law.

(3) "Cyberbullying" and "harassment, intimidation or bullying

(4) "De-Identified Information" means any Personally, Identifiable Information about a reporter and the name, name, phone number, physical address, and email address of the subject(s) of a report.

(5) "Local law enforcement contact" means a local law enforcement officer designated by the Department of State Police to be notified when the tip line receives a report of a threat to student safety or potential threat to student safety.

(6) "Personally, Identifiable Information" means any information that would permit the identification of the person as a person reporting information to the SSTL. It includes, but is not limited to, name, phone number, physical address, email address, and information that identifies the machine or device from which the person made the report.

(7) “Service provider” means a person designated by the department to be notified when the tip line receives a report of a threat to student safety or potential threat to student safety. “Service provider” includes:

(a) A provider of behavioral health care or mental health care;

(b) A provider of school-based health care;

(c) A certificated school counselor;

(d) A clinical social worker licensed

(e) A professional counselor or a marriage and family therapist licensed

(8) “Student” means a student of:

(a) A school district,

(b) A community college,

(c) A private school that provides educational services to kindergarten through grade 12 students;

(d) A public charter schools

(e) A career school,

(f) A public university

(9) “Threat to student safety” includes, but is not limited to, a threat or instance of:

(a) Harassment, intimidation, or bullying or cyberbullying;

(b) Suicide or self-harm; and

(c) Violence against others.

(10) “Tip” means reports of information concerning threats to student safety or potential threats to student safety made by phone call, text message, email, web-form submission, or an application on a mobile device submission accepted by the SSTL.

(11) “Tip line” means a statewide resource designed to accept information concerning threats to student safety or potential threats to student safety through methods of transmission including:

(a) Telephone calls;

(b) Text messages;

(c) Electronically through the Internet; and

(d) Use of an application on a mobile device.

(12) “Tip Line Technician” means contracted staff who receive, route and ensure follow-up occurs for calls, e-mails, text messages, and online tips 24 hours a day, seven days a week.

EXHIBIT C

- **Responsibilities.**

(1) University of Montana Safe School Center is responsible for:

(a) Establishing a tip line for students and other members of the public to confidentially report information concerning threats or potential threats to student safety;

(b;

(c) Following any applicable laws and rules;

(d) Analyzing and interpreting data entered into the SSTL to help schools improve their response to safety issues;

(e)

(f) Coordinating outreach and programmatic support to schools, school districts, Education Service Districts, law enforcement agencies and service providers involved in or entering the program;

(g) Establishing a process for documenting the closure of tips and ensuring that the process is being used.

(h) Generating analysis, reports and studies. Analysis, reports and studies shall contain only aggregated information and shall not contain any information that personally identifies reporters or any students. Reports may contain aggregated information concerning how referrals were handled by local law enforcement and service providers and the outcomes of the referrals.

(i) Ensuring training materials explain that reporters may make an anonymous report or, if they identify themselves, how their identity is protected and how it may be shared as set out in.

EXHIBIT D

(2) The SSTL vendor contracted by the University of Montana Safe School Center is responsible for:

(a) Receiving SSTL tips via phone, email, application on a mobile device, website submission and text message and processing those tips;

(b) Ensuring adequate staffing of Tip Line Technicians to handle tip volume;

(c) Ensuring SSTL is functional and capable of operation 24 hours per day, seven days per week;

(d) Providing SSTL database access and the ability to extract de-identified data for analysis to designated persons authorized by the University of Montana Safe School Center;

(e) Following up on reported tips and documenting the status of tips through the SSTL;

(f) Prompting schools to provide updated responsible staff and service provider, if applicable, contact information on a regular basis;

(g) Providing physical and online information security protection including administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

(h) Ensuring Tip Line Technicians have the requested qualifications, training, and experience in taking crisis calls.

(i) Maintaining a policy and procedure manual that contains specific protocols to be used depending on the nature of the tip as well as general procedures regarding interviews and taking information.

EXHIBIT E

(3) The schools, school districts or Education Service Districts are responsible for:

(a) Determining, keeping current, and providing to the SSTL lists of responsible staff and service providers capable of handling tips relayed to the school, school district or Education Service District by the SSTL;

(b) Verifying the authenticity and validity of received reported threat to student safety or potential threat to student safety;

(c) Forwarding tip information to law enforcement or service providers as appropriate;

(d) Following up on assigned tips, providing information about updates and outcomes to the SSTL to the extent not prohibited by any applicable federal or state confidentiality provisions, and closing tips through the SSTL.

SIGNATURES

SPRIGEO_____ Date_____

MSSC_____ Date_____

Browning School District #9_____ Date_____