

ATTACHMENT D
CONFIDENTIALITY, PRIVACY, AND SECURITY ADDENDUM

This Confidentiality, Privacy and Security Addendum (“Addendum”) is hereby incorporated into the Marmot Library Network Service Agreement between Mesa County Valley School District No. 51 (“District”) and Marmot Library Network, Inc. effective as of July 1, 2016 (the “Agreement”). This Addendum shall be part of the Agreement. For purposes of this Addendum, Marmot is referred to as “Contractor.”

RECITALS:

- A. District wishes to disclose certain information to Contractor pursuant to the work being performed by Contractor, some of which may constitute Education Records and/or Student Personally Identifiable Information (defined below); and
- B. Contractor agrees to protect the privacy and provide for the security of Education Records and Student Personally Identifiable Information disclosed to Contractor pursuant to the Agreement, in accordance with the terms of this Addendum.

Therefore, the parties agree as follows:

A. Definitions

1. "Aggregate Data" means data collected or reported at a group, cohort or institutional level that is derived, in whole or in part, from Education Records or PII and is aggregated to preserve anonymity of each individual included in the data.
2. "Destroy" means to remove Student Personally Identifiable Information from Contractor’s systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in NIST Special Publication 800-88 Guidelines for Media Sanitization so that the Student Personally Identifiable Information is permanently irretrievable in the Contractor’s and Subcontractor’s normal course of business.
3. “Education Records” means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm or microfiche, that (a) is directly related to a District student, past or present; (b) is maintained by the District or by any party acting for or on behalf of the District; and (c) is subject to state and/or federal privacy laws, rules and regulations, including but not limited to, those specified in §B. 2. of this Addendum.
4. “Incident” means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a District or Contractor system or Student Personally Identifiable Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a District system for the processing or storage of data; (iv) a material breach of the Agreement that involves the misuse or unauthorized release of Student Personally Identifiable Information; or (v) changes to District system hardware, firmware, or software characteristics without District’s knowledge, instruction, or consent.
5. "Student Personally Identifiable Information" or "PII" means information 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 Contractor or any Subcontractor. Student Personally Identifiable Information includes, but is not limited to a student's name; the name of a student's parent or other family member; the address of a student or student's family; a personal identifier such as a student's social security number, student number, or biometric record; other indirect identifiers such as a student's date of birth, place of birth, and mother's maiden name; a student’s email address, cell phone number or any other information that allows physical or online contact with a student; a student’s discipline or criminal records; a student’s juvenile dependency records; a student’s medical or health records including, without limitation, records regarding a student’s disabilities; a student’s socioeconomic information, political affiliations, or religion; a student’s text messages, IP address, or online search activity; a student’s photos and voice recordings; a student’s food purchases; or geolocation information. PII also includes other information that, alone or in combination, is linked 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 educational agency or institution reasonably believes knows the identity of the student to whom the information relates.
6. “Subcontractor” means any third party engaged by Contractor to perform or aid in performance of one or more of the Contractor’s obligations under the Agreement, or any third party engaged by a Subcontractor to perform or aid in performance of one or more of the Subcontractor’s obligations to Contractor.
7. “Targeted Advertising” means selecting and sending advertisements to a student based on information obtained or inferred over time from the student’s online behavior, use of applications, or PII. Targeted Advertising does not include advertising

to a student at an online location based on the student's current visit to that location or in response to the student's request for information or feedback and is without the collection and retention of a student's online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

B. General Provisions

1. The District reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to Education Records and the information and data contained therein, including PII, and all related data and content. All Education Records and PII disclosed or provided to or used by Contractor under the Agreement shall remain at all times the property of the District.
2. Contractor shall comply with all laws and regulations concerning confidentiality of Education Records and any and all PII contained therein, including, but not limited to, the Family Educational Rights and Privacy Act of 1974, as amended ("FERPA"), 20 U.S.C. Section 1232g, FERPA's implementing regulations set forth at 34 C.F.R. Part 99, and the Student Data Transparency and Security Act, §22-16-101 *et al.*, C.R.S (the "Act").
3. Contractor shall immediately forward to the District's Superintendent any request or demand from a third party for Education Records or PII in the possession of Contractor.
4. Upon request of the District, Contractor shall submit its data processing facilities for an audit of the measures referred to in this Addendum by the District or its authorized representative.
5. Contractor shall send the District a written notice, which includes a clear explanation of the proposed changes prior to making a material change to Contractor's privacy policies.
6. During the term of the Agreement, Contractor shall be considered a "School Official" (as that term is used in FERPA and its implementing regulations) of the District to the extent it maintains, receives, uses, stores, manages, manipulates or provides access to Education Records or PII under the Agreement or assists the District with such functions. The parties acknowledge and agree that Contractor (i) is performing under the Agreement services and functions that the District would otherwise perform using its own employees; and (ii) is under the District's direct control with respect to the use and maintenance of Education Records and PII.
7. With respect to Education Records or PII which Contractor is exposed to or which is transmitted, accessed, kept, maintained or received by Contractor pursuant to this Agreement, Contractor shall:
 - a. Comply with all such state and federal laws, rules and regulations which apply to the District related to Education Records and PII, including FERPA and the Act; and
 - b. Maintain the privacy and confidentiality as required by law of all Education Records and PII; and
 - c. Not use, transfer, sell or disclose any such Education Records or the PII contained therein except as necessary to carry out its obligations under this Agreement or as required or permitted by law; and
 - d. Not at any time use or seek to use any of the Education Records or PII acquired during the term of this Agreement for Contractor's own benefit or for the benefit of any other person or entity other than the District; and
 - e. Maintain adequate and appropriate policies and procedures to ensure the privacy and security of Education Records and PII as required by law; and
 - f. Require its Subcontractors, agents and employees that are or may be exposed to Education Records or PII, to comply with the terms of this Addendum.
8. The terms of this Addendum shall survive the termination of the Agreement. Violation of this Addendum shall constitute a breach of the Agreement.

C. Subcontractors

Contractor shall not use a Subcontractor or disclose Education Records or PII contained therein to a Subcontractor unless and until the Contractor contractually requires the Subcontractor to comply with C.R.S. §§22-16-108 through 22-16-110 and the requirements of this Addendum.

1. If Contractor discovers that a Subcontractor has committed a material breach of the Agreement between Contractor and Subcontractor that involves the misuse or unauthorized release of Education Records or PII, the District may terminate the Agreement unless Contractor terminates the Agreement with Subcontractor as soon as possible after Contractor knows or has reason to know of Subcontractor's material breach.
2. Upon discovering the misuse or unauthorized release of Education Records or PII held by a Subcontractor, Contractor shall notify District within one calendar day, regardless of whether the misuse or unauthorized release by the Subcontractor is a result of a material breach of the terms of the Agreement or results in an Incident.
3. No later than thirty (30) days after the signing of the Agreement, Contractor will provide the District with information detailing the purpose and the scope of the Agreement between the Contractor and all Subcontractors and the types and uses of Education Records and/or PII that Subcontractor(s) may possess, store, receive, disclose, share or have access to under the Agreement between the Contractor and Subcontractor(s).
4. Contractor shall not maintain or forward Education Records or PII to or from any other facility or location except for backup and disaster recovery purposes. Any backup or disaster recovery contractor shall be considered a Subcontractor that must comply with the Subcontractor requirements in this Addendum.

D. End of Agreement

1. If Contractor violates the terms of this Addendum and such non-compliance results in the misuse or unauthorized release of Education Records or PII by the Contractor or any third party, the District may terminate the Agreement immediately by written notice to Contractor.
2. Upon request by the District made before or within thirty (30) calendar days after termination of the Agreement, Contractor shall make available to the District a complete and secure (i.e. encrypted and appropriately authenticated) download file of all data, including, but not limited to, all Education Records, PII, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format.
3. Unless otherwise directed by the District in writing, Contractor shall, within thirty (30) calendar days following the termination of this Agreement, Destroy all Education Records and PII it has stored, acquired, collected, generated, or inferred during the term of this Agreement or in connection with its performance of its obligations under this Agreement. The Contractor shall notify the District of the date upon which all of the Education Records and PII are Destroyed.
4. The District shall at all times have and reserve the right to use Contractor's established operational services to access and retrieve Education Records and/or PII stored on Contractor's infrastructure at its sole discretion.

E. Use

1. The Contractor shall not access, use or share Education Records or PII except as necessary to perform its responsibilities specified in the Statement of Work set forth in Exhibit A of the Agreement. However, Contractor may use PII to maintain, develop, support, improve, or troubleshoot Contractor's website, online service, online application, or mobile application, to the extent provision of such website, service or application is necessary to perform the Statement of Work.
2. In the event the Agreement requires Contractor to store, process or transfer Education Records or PII, Contractor shall store, process, and transfer Education Records or PII only in or to facilities located within the United States.
3. Contractor may use Education Records or PII in a manner that is not specified in the Statement of Work set forth in Exhibit A of the Agreement without violating the terms of this Addendum provided that the use does not involve selling or using PII for Targeted Advertising or creating a personal profile of the student, and the use is limited to one or more of the following purposes:
 - a. To ensure legal or regulatory compliance.

- b. To comply with a valid court order or other lawful judicial process.
- c. To protect the safety of users or others on Contractor's website, online service, online application, or mobile application.
- d. To investigate a matter related to public safety.

If Contractor uses or discloses Education Records or PII in accordance with this Section D.3., Contractor shall notify the District within two calendar days of the use or disclosure of the Education Records or PII.

- 4. At any time during the term of this Agreement, the District may submit to Contractor a written request that Contractor Destroy Education Records or PII collected, generated or inferred regarding one or more District students as a result of the Agreement. Upon receipt of such request, the Contractor shall Destroy the Education Record(s) or PII that is the subject of the request as soon as practicable after the date of the request unless:
 - a. The Contractor obtains the written consent from the parent(s) or legal guardian(s) of such student(s) or from the student(s) (if the student(s) is/are over the age of 18); or
 - b. The student(s) has transferred to another public school that requests that the Contractor retain the student's Education Record or PII.

F. Incident

- 1. If Contractor becomes aware of an Incident, misuse of PII or Education Record(s), or unauthorized disclosure involving any PII or Education Record(s), it shall notify the District within one (1) calendar day and consult and cooperate with the District regarding appropriate remediation, mitigation and recovery measures, and with law enforcement agencies to whom the Incident, misuse or disclosure is reported, if any.
- 2. Unless Contractor can establish that Contractor or any of its Subcontractors is not the cause or source of the Incident, Contractor shall be responsible for the cost of notifying each individual (or parent/guardian, as applicable) whose PII may have been compromised by the Incident.
- 3. Contractor shall determine the cause of an Incident and produce a remediation plan to address and resolve the Incident and reduce the risk of incurring a similar type of Incident in the future. Contractor shall present its analysis and remediation plan to the District within ten (10) calendar days of notifying the District of an Incident. The District reserves the right to adjust this plan, in its sole discretion. If Contractor cannot produce its analysis and plan within the allotted time, the District, in its sole discretion, may perform such analysis and produce a remediation plan, and Contractor shall reimburse the District for the reasonable costs thereof.
- 4. Contractor shall indemnify, defend, and hold harmless the District, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred, that arise out of or as a result of any Incident, or any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees in violation of the terms and conditions of this Addendum. Notwithstanding any other provision of this Agreement, Contractor shall be liable to the District for all direct, consequential, and incidental damages arising from an Incident caused by Contractor or its Subcontractors.
- 5. In the event of an Incident, Contractor shall provide the District or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating, or resolving the Incident.

G. Prohibited Activities

A Contractor that uses, creates, or acquires Education Records or PII shall not knowingly engage in any of the following activities:

- 1. Contractor shall not collect, use or share Education Records or PII for any purpose not specifically authorized by the Agreement. Contractor may use Education Records or PII for a purpose not expressly authorized by the Agreement only with the written consent of the District and with the written consent of the student(s) that are the subject of (provided that the student is over the age of 18) or the student's parent or legal guardian.

2. Contractor shall not share, transmit, report or disclose Aggregate Data to any third party or publically release Aggregate Data without the prior written authorization of the District, which authorization may be withheld if the District determines, in its absolute discretion, that such data was not aggregated using protocols that are effective for preserving the anonymity of each individual included in the data or that the proposed release or disclosure is otherwise contrary to applicable law or regulations regarding Education Records or PII. Any release, disclosure or reporting of Aggregate Data by Contractor that occurs without the District's prior written authorization shall be considered an Incident, and shall be a misuse of Education Records or PII, or unauthorized disclosure of PII, in violation of this Addendum.
3. Contractor shall not use or disclose Education Records or PII to any third party in a manner that is materially inconsistent with the Contractor's privacy policy, except as stated in subsection 3, below, of this Section G.
4. Contractor shall not sell PII, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of the Contractor, or any assets of the Contractor, by another entity, so long as the successor entity continues to be subject to the provisions of this Agreement.
5. Contractor shall not use or share PII with any party for the purposes of Targeted Advertising to students.
6. Contractor shall not use PII to create a personal profile of a student unless expressly authorized to do so in the Agreement or such use has been authorized in writing by the student (if the student is over the age of 18) or the student's parent or legal guardian.

H. Data Security

1. Contractor shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of Education Records and PII. At a minimum, the information security program shall include the requirements listed in this Section H – Data Security.
2. Contractor shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Agreement. Contractor shall take full responsibility for the security of all Education Records and PII in its possession, and shall hold the District harmless for any damages or liabilities, including court costs, litigation expenses and attorneys' fees, occasioned by or resulting from the unauthorized disclosure or loss thereof. Contractor shall provide for the security of such Education Records and PII, in a form acceptable to the District, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.
3. Contractor shall provide the District or its designated representatives with access, subject to Contractor's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of Education Records and PII, maintaining District systems, and evaluating physical and logical security control effectiveness.
4. Contractor represents and warrants that (i) no direct services of any kind or nature shall be provided to any District student under this Agreement; and (ii) no employee, Subcontractor or agent of Contractor shall have regular contact with any District student during the course of providing services under the Agreement. "Regular contact," as used in this paragraph, shall mean contact or communication that is not incidental and occurs at least once per month.
5. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.
6. Contractor shall protect all PII with a complex password. Contractor shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Contractor shall periodically change passwords and shall ensure passwords are not reused. Contractor shall have password locks for laptops and mobile devices.
7. Contractor shall routinely assess account inactivity for potential stale accounts and disable and/or immediately delete unused and terminated user accounts.
8. Contractor shall not share PII on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes. Hard copies containing PII must be physically secured and not left unattended, and Destroyed after authorized use is completed.

9. Contractor shall implement annual intrusion penetration/vulnerability testing.
10. Contractor shall encrypt PII in transit and shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Contractor shall encrypt disks and storage for all laptops and mobile devices.
11. Contractor shall provide annual, mandatory security awareness and PII handling training for all of its employees/Subcontractors handling PII pursuant to this Agreement.
12. Contractor shall install and maintain on computers accessing or processing PII appropriate endpoint security anti-virus, anti-ransomware and anti-malware software. Contractor shall ensure all Contractor's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.
13. Contractor shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit PII. Contractor shall never send PII or Education Records via email or transport PII or Education Records on removable media.
14. Contractor shall have physical security in buildings housing PII or Education Records, along with controlled physical access to buildings and/or data centers.
15. Contractor's devices used to copy or scan hard copies of PII or Education Records must have encrypted storage. Contractor shall scrub storage devices when equipment is retired.
16. Contractor shall protect PII stored in cloud-based systems in the same manner as local PII. Use of free cloud-based services is prohibited. Contractor shall use secondary encryption to protect PII in cloud storage. Cloud environments, when employed by Contractor, must be fully documented by Contractor and open to District inspection and verification. Access to Contractor's cloud-based computing environments is only permitted via restricted access, by VPN or privileged access lists, and shall not be accessible directly via the Internet.

I. Transparency Requirements

1. Contractor shall facilitate District access to and amendment of any Education Records or PII in Contractor's possession or under its control as needed for the District to comply with FERPA or other applicable state or federal law.
2. Contractor understands and agrees that the District may post and maintain on its website a list of the District's school service providers that includes Contractor, as well as a copy of the Agreement, including this Addendum.
3. Contractor shall post and maintain the following information on its public website:
 - a. Contact information for an individual within Contractor's organization that can provide information on or answer questions related to the use of PII by Contractor.
 - b. An explanation of how PII will be shared with Subcontractors or disclosed to any third party.
 - c. The types of PII that are collected, generated, or used by the Contractor. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate.
 - d. An explanation of the PII, an explanation of how the PII is used, and the learning purpose for which the PII is collected and used.

Contractor shall update the above-listed information on its website as necessary to assure that the information provided is accurate and current.