DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is attached to and forms a part of the Contractor's Product Terms and End User License Agreement available at https://www.goguardian.com/policies/eula (as may be amended from time to time in accordance with the terms therein) (the "Contract") by and between Weld County School District 6 ("District") and Liminex, Inc dba GoGuardian ("Contractor") (the Addendum and the Contract are collectively referred to hereinafter as "Agreement"). This Addendum supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. 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 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 "Contractor Parties" means Contractor, its affiliates, licensors, and suppliers, and their respective officers, directors, employees, shareholders, agents and representatives.

1.2 "*Designated Representative*" means the District or Contractor employee(s) specified on Schedule 1 designated by each party in a writing to the other to whom all notices required in this Addendum will be sent.

1.3 "*District Data*" means student information provided to Contractor by or at the direction of District, or to which Contractor has access in the course of Contractor's performance of the Services under the Contract. District Data includes, but is not limited to, "Personal Identifying Information" as defined by C.R.S. § 24-73-101(4)(b), "Personally Identifiable Information" and "Education Records" as defined by 20 U.S.C. § 1232g and 34 C.F.R. § 99.3, student data, metadata, and user content.

1.4 "*De-identified Data*" means District Data from which all Personal Identifying Information and Personally Identifying Information have been permanently removed so that no individual identification can be made.

1.5 "*End User*" means individuals authorized by the District to access and use the Services provided by the Contractor under the Contract.

1.6 "*Security Incident*" means the unauthorized disclosure of or access to District Data.

1.7 "*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) SP 800-88 Guidelines for Media Sanitization, as amended so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.8 "*Services*" means the technology services set forth in the Contract and other technology products or services that the Contractor may provide to the District now or in the future.

1.9 "*Subcontractor*" means a party other than the Contractor that the Contractor uses to provide the Services and who has access to District Data.

2. Ownership and Access to District Data

2.1 District Owns District Data and De-identified Data. District owns all rights, title, and interest in and to District Data and De-identified Data, and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto. 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 or as otherwise specified in this Agreement. The District further grants to Contractor a perpetual, nonexclusive license to use De-identified Data solely for the purpose set forth in Section 3.2. Contractor shall have no rights, title, or interest, implied or otherwise, to District Data or De-identified Data except as expressly stated in this Agreement. Provided, however, that except for such District Data and De-identified Data, Contractor owns all rights, title and interest (including, but not limited to all copyright, patent, trademark and trade secret rights) in its Services and intellectual property.

2.2 Contractor Access to Education Records. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement and in accordance with the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it is designated as a "school official" with "legitimate educational interests" in the Education Records and Personally Identifiable Information disclosed pursuant to the Contract, and Contractor agrees to comply with FERPA limitations and requirements imposed on school officials. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the Family Policy Compliance Office.

2.3 Employees. Contractor shall require its employees who have access to District Data to comply with this Addendum. Contractor shall be responsible for its employees' noncompliance with the terms of this Addendum.

2.4 Subcontractors. Contractor shall enter into written agreements with its Subcontractors whereby the Subcontractors agree to protect District Data in a manner consistent with the terms of this Addendum. Contractor is responsible for any Subcontractor noncompliance with the terms of this Addendum.

2.5 Parent/Guardian/Student Access to District Data. In accordance with FERPA, District has established reasonable procedures by which a parent, legal guardian, or eligible student may review and request to amend Education Records. Contractor shall respond within twenty (20) days to, and cooperate with, a District request to review or amend Education Records held by the Contractor and not accessible by the District. In the event that a parent, legal guardian, or eligible student contacts the Contractor to review or request to amend Education Records held by the Contractor, the Contractor shall refer such individuals to the District.

2.6 Third Party Access to District Data. If a third party, excluding a parent/guardian/student or Subcontractor, contacts Contractor to request District Data held by the Contractor pursuant to the Agreement, then the Contractor shall redirect such third-party request to the District; provided, however, that if the request is a subpoena or other process issued to the Contractor from a court of competent

jurisdiction, then prior to compliance, Contractor shall (unless prohibited by law) provide the District with prompt notice of such request to allow the District to seek a protective order.

2.7 Process Received by the District. If the District receives a subpoena or other process issued from a court of competent jurisdiction for District Data held by the Contractor and not accessible by the District, then the District shall promptly notify the Contractor and the Contractor shall produce the responsive District Data to the District in a manner and within a timeframe that allows the District to comply with the subpoena or process.

2.8 District Access to District Data. The District shall have the right to access and retrieve District Data stored by or in possession of Contractor and not accessible by the District upon written notice to Contractor's Designated Representative. Contractor shall make the requested District Data available to the District within ten (10) days from the date of request unless the parties mutually agree to a different timeframe.

3. Data Use

3.1 Authorized Use. Contractor shall collect and use District Data solely for the purpose of fulfilling its duties and providing the Services under the Agreement, and for improving the Services under the Agreement. Except as expressly permitted by the Agreement, all other Contractor uses of District Data shall be prohibited, including, but not limited to: (i) selling or renting District Data, (ii) mining District Data; (iii) using District Data for marketing, advertising, or other commercial efforts by Contractor, and (iv) developing a profile of a student, parent, guardian, family member, or District employee for any commercial purpose other than providing the Services to the District.

3.2 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of the Services, and/or the development of new products and services, as a party would be able to use de-identified data pursuant to 34 C.F.R. § 99.31(b). Contractor shall not re-identify or attempt to re-identify any De-identified Data and shall not transfer De-identified Data to any third party unless (i) such party agrees in writing not to re-identify or attempt to re-identify the De-identified Data, and (ii) that party agrees to comply with applicable law.

3.3 Modifications of Terms of Service. Contractor shall provide notification of material changes to its terms of service, including without limitation its privacy policies, in a timely manner to District.

4. Data Security

4.1 Data Security. Contractor shall employ administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of, and designed to prevent the unauthorized disclosure and destruction of District Data in the possession or under the control of Contractor which are (a) no less rigorous than those maintained by Contractor for its own information of a similar nature, (b) no less rigorous than the controls and practices put forth in the National Institute of Standards and Technology Cyber Security Framework, as amended; and (c) required by applicable law. These measures shall include, but not be limited to:

4.1.1 Encryption. Encryption of District Data at rest and in transit in accordance with NIST Special Publication 800-57, as amended;

4.1.2 Technical Safeguards. The use of appropriate procedures and technical controls regulating data entering Contractor's network from any external source;

4.1.3 Physical Safeguards. Physical security measures, including, without limitation, securing District Data within a secure facility where only authorized personnel and agents will have physical access to District Data;

4.1.4 Administrative Safeguards. User identification and access controls designed to limit access to District Data to authorized users;

4.1.5 Employee Training. Conduct of periodic employee training regarding the security measures referenced in this Section.

4.1.6 Periodic Risk Assessment. Conduct of periodic risk assessments and remediation of any identified security vulnerabilities as appropriately determined by Contractor.

4.1.7 Audit Trails. Use of reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity.

4.2 Review and Verification of Safeguards. Contractor, at Contractor expense, shall periodically conduct a review of its security safeguards in connection with the Services and prepare a report (the "Audit Report"). No more than once per year during the term of the Agreement, District shall have the right to request and receive an executive summary of the Audit Report and to share it with its auditors and regulators; provided, however, that the executive summary of the Audit Report shall be subject to the confidentiality provisions in the Contract, if any.

5. Security Incident

5.1 Security Incident. If Contractor becomes aware of any actual or reasonably suspected Security Incident, then Contractor shall (i) promptly notify District, in writing, of the occurrence of such Security Incident, including, the nature of the incident, a description of the District Data subject to unauthorized access or disclosure, and the individuals impacted; (ii) promptly supplement the written notification set forth in Section 5.1(i) as new information becomes available; (iii) investigate and conduct a reasonable analysis of the cause(s) of such Security Incident; (iv) provide periodic updates of any ongoing investigation to the District; (v) develop and implement an appropriate plan to remediate the cause of such Security Incident to the extent such cause is within Contractor's control; and (vi) reasonably cooperate with District's reasonable investigation or efforts to comply with any notification or other regulatory requirements applicable to such Security Incident as required by law.

5.2 Reimbursement of Costs. In the event of a Security Incident caused by Contractor's breach of this Addendum, then in addition to any other remedies available to the District, Contractor shall reimburse District for the actual costs incurred by the District in investigating, responding to, and remediating such Security Incident, including, the cost of (i) providing notice to affected parents of students, (ii) providing one-year's credit monitoring services to affected individuals; (iii) reasonable legal fees; (iv) reasonable audit costs; and (vi) fines and penalties. Contractor shall reimburse District for the foregoing costs within thirty (30) days of receiving an undisputed invoice therefor.

5.3 Effect of Security Incident. The District may require Contractor to suspend all Services pending the investigation and successful resolution of any Security Incident. If the Security Incident caused by Contractor constitutes a breach of the Agreement, then the District may terminate the Agreement and receive a refund of any prepaid, unused fees, including without limitation, prepaid fees associated with the period of suspension.

6. Compliance with Law

6.1 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" as defined in, and shall comply with, the Colorado Student Data Transparency and Security Act, C.R.S. § 22-16-101 et seq. To the extent not previously provided, within ten (10) calendar days after signing this Addendum, Contractor shall provide to the District in the format specified in Schedule 3 or in a format that is easily accessible through Contractor's website in language easily understandable to a layperson: (a) the data elements of District Data that Contractor collects, generates or uses pursuant to the Contract; (b) the educational purpose for which Contractor collects and uses the District Data; (c) Contractor's policies regarding retention and disposal of District Data; (d) how Contractor uses, shares or discloses the District Data; and (e) a statement whether Contractor's Contract has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth herein. Contractor shall update this information as necessary to maintain accuracy. The District reserves the right to terminate the Agreement, as specified in Section 7, should the District receive information after the Effective Date that significantly modifies Contractor's representations made in this Section 6.1.

6.2. Children's Online Privacy and Protection Act. In performance of the Services required by the Contract, 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, 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 full notice of its collection, use, and disclosure practices.

6.3 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 without limitation COPPA; FERPA; the Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; the Colorado Student Data Transparency and Security Act; and the Colorado Consumer Protection Act, C.R.S. §§ 6-1-101 to 6-1-1214, 24-73-101 to 103.

7. Term and Termination

7.1 Term. This Addendum will become effective when the Contractor has executed this Addendum ("Effective Date"). Subject to earlier termination as provided in the Agreement, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties.

7.2 Termination by the District. In addition to its termination rights under the Contract and except as set forth in Section 7.3, the District may terminate the Agreement if the Contractor breaches a material term of this Addendum and such breach is not cured within thirty (30) days of Contractor's receipt of written notice of such breach. Notwithstanding the foregoing, to the extent such breach cannot be remedied, District may terminate the Agreement on less than thirty (30) days' written notice.

7.3 Termination by the District for Misuse of District Data. If the Contractor is a "school service contract provider" as defined in Section 6.1 of this Addendum, and breaches a material term of the Agreement that involves the misuse or unauthorized release of student Personally Identifiable Information, the District may terminate the Agreement in accordance with the Colorado Student Data Transparency and Security Act and District policy.

8. Data Destruction Upon Termination or Expiration

8.1 Destruction of District Data. Unless otherwise provided in the Contract, within thirty (30) days of the termination or expiration of the Agreement and upon written request, Contractor shall Securely Destroy, or caused to be Securely Destroyed, District Data in its possession or under its control, including without limitation District Data in the possession or under the control of its Subcontractors. Upon written request, the Contractor shall promptly certify in writing to District that such District Data has been Securely Destroyed using the form attached hereto as Schedule 2.

8.2 Response to Specific Data Destruction or Return Requests. Contractor shall Securely Destroy or return any specific District Data in its possession or under its control within ten (10) business days, excluding national holidays, after receiving a written request from the District.

9. Indemnification and Limitation of Liability

Contractor shall indemnify and hold District and its directors, employees, and agents harmless from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, award, penalties, fines, costs or expenses actually incurred, including reasonable attorneys' fees, arising out of or resulting from any third-party claim against District or its directors, employees, and agents arising out of or resulting from Contractor's negligent or intentional act or omission in the performance of its obligations set forth in this Addendum, or the negligent or intentional acts or omissions of Contractor's employees or agents. Neither party (including Contractor Parties) will be liable to the other for any indirect, special or consequential damages of any kind arising out of this Agreement, whether based on breach of contract, tort (including negligence) or otherwise, whether or not such party has been advised of the possibility of such damage. In no event shall Contractor Parties' (including Contractor's) total liability hereunder (for any cause, including in tort) exceed three (3) times the amount of District's payment to Contractor for the Services giving rise to such claim for the calendar year in which such claim arose.

10. Insurance

10.1 Type. In addition to the insurance required by the Contract, if any, Contractor shall purchase and maintain during the term of this Agreement Technology Errors and Omissions/Professional Liability Insurance, including Network Security and Privacy Liability Insurance. Such policies shall cover professional misconduct or lack of ordinary skill in providing services, systems and/or product as defined in the scope of services of this Agreement.

10.2 Additional Requirements. In addition to the foregoing requirements, the policies set forth in Section 10.1 shall, except for professional liability policies, shall be endorsed to include the following additional insured language: Weld County School District 6, and its elected officials, trustees, employees, and agents, shall be named as additional insureds with respect to liability arising out of the activities performed by, or on behalf of the Contractor." The policy shall be for the following amounts:

Minimum Limits:		
Per Loss	$	1,000,000
Aggregate	$	3,000,000

11. Miscellaneous

11.1 Conflict with End User Agreements. 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, the parties agree that in the event of a conflict between the terms of any such agreement and the Agreement, the terms of this Addendum and the Contract, in that order of precedence, shall control.

11.2 Survival. The Contractor's obligations under Sections 2, 3, 4, 5, 8, 9, and 11 shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

11.3 Governing Law. The Agreement shall be governed and construed in accordance with the laws of Colorado, excluding its choice of law rules. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the federal court located in Colorado or the state court located in Weld County, Colorado.

11.4 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*.

11.5 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District, except in connection with a merger, consolidation or sale of substantially all of Contractor's assets, District Data may be transferred to the successor entity provided this Addendum is binding on such successor entity.

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

11.7 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 -- Certification of Destruction\Return of District Data

11.8 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. For purposes of executing this Agreement, facsimile or scanned signatures shall be as valid as the original.

[Signatures appear on next page.]

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date set forth below each party's signature.

Weld County School District 6

By: Mandy Hydock, Director of Finance

Date: Oct 4, 2021

Contractor

By: DocuSigned by: Michael Jonas 6CD8C493E787445...

Michael Jonas CFO

Date: 10/10/2021

SCHEDULE 1

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: Mandy Hydock **Title:** Finance Director **Address:** 1025 9th Avenue Greeley, CO 80631 **Phone:** 970-348-6000 **E-mail:** mhydock@greeleyschools.org	**Name:** Legal Department **Title:** **Address:** 2030 E Maple Ave, Suite 100 El Segundo, CA 90245 **Phone:** **E-mail:** legal@goguardian.com

SCHEDULE 2
Certification of Destruction

I, _____[NAME]_____, as the authorized representative of the Contractor, do hereby acknowledge and certify under penalty of perjury that:

Part A - Destruction:

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

_____ the District Data provided to Contractor's Subcontractors pursuant to the Agreement in accordance with federal and state law was destroyed as set forth below:

Contractor Name: _____
Contractor Representative Name: _____
Title: _____
Signature: _____ Date: _____