Master Terms and Conditions

THESE MASTER TERMS AND CONDITIONS ("MASTER TERMS") SHALL APPLY TO THE AGREEMENT ENTERED INTO BETWEEN THE DISTRICT AND THE COMPANY, PURSUANT TO THE SALES CONTRACT, IN WHICH THESE MASTER TERMS ARE HEREBY EXPRESSLY INCORPORATED.

This agreement is between ESGI, LLC (Company) and **Raytown Quality Schools** (District).

1. **Indemnity.** Company agrees to indemnify and hold harmless the District from, against and in respect to any and all claims, losses, or liabilities involving a claim or action brought against the District by a third party for damages incurred or suffered, directly or indirectly, arising from or relating to web-based progress monitoring software, as is contemplated under this Agreement.

2. **Force Majeure.** If either party is prevented from performing any of its obligations due to any cause which is beyond the non-performing party's reasonable control, including fire, explosion, flood, epidemic/pandemic or other acts of God; acts, regulations, or laws of any government; strike, lock-out or labor disturbances; or failure of public utilities or common carriers (a "Force Majeure Event"), such non-performing party shall not be liable for breach of this Agreement with respect to such non-performance to the extent any such non-performance is due to a Force Majeure Event. Such non-performance will be excused for three months or as long as such event shall be continuing (whichever occurs sooner), provided that the non-performing party gives immediate written notice to the other party of the Force Majeure Event.

3. **Disputes.** To the extent allowed by applicable law, any controversy or claim arising out of or relating to this Agreement or any breach thereof, shall be settled by informal mediation with the parties subject to this Agreement. If any controversy cannot be resolved through informal mediation, any legal action in connection with this Agreement shall be filed in the Circuit Court of Jackson County, Missouri, or the United States District Court for the Western District of Missouri, as appropriate, to which jurisdiction and venue Company expressly agrees. The prevailing party in any such action shall be entitled to recover attorney's fees and court costs from the non-prevailing party.

4. **Termination for Cause.** District may terminate the Agreement for cause if Company:

   (1) repeatedly refuses or fails perform the act(s) described in the Sales Contract or the Data Governance Addendum;
   (2) engages in conduct that triggers grounds for termination, as contemplated by the Data Governance Addendum;
   (3) repeatedly disregards applicable laws, statutes, ordinances, codes, rules and regulations, or lawful orders of a public authority;
   (4) engages in conduct that would constitute a violation of state or federal criminal law, including but not limited to, laws prohibiting certain gifts to public servants, or engages in conduct that would constitute a violation of the District's ethics or conflict of interest policies or District's Board of Education's policies; or
   (5) Otherwise is guilty of a substantial breach of a provision of this Agreement.

5. **Termination for Convenience.** District may terminate the Agreement at any time by giving at least ten (10) days' notice in writing to Company. If the contract is terminated by the District as provided herein, the District will pay Company for any proven unrecoverable loss with respect to

materials, equipment, or purchases made or utilized pursuant to this Agreement, to the extent of actual loss thereon, by the date of termination.

6. **Compliance with Laws and District Board Policy.** Company, at Company's sole cost, shall comply with all present and future laws, ordinances, rules, regulations and District Board Policy.

7. **Children's Online Privacy Protection Act.** The parties recognize and agree that with respect to the Children's Online Privacy Protection Act ("COPPA"), the District gives its consent to Company on behalf of parents of children from whom any personal information shall be gathered, as contemplated under the Agreement. As the agreement only contemplates the collection of personal information from children under the age of thirteen (13) for educational purposes, for the use and benefit of the school, and for no other commercial purpose, the parties recognize that COPPA does not require that the Company obtain consent from parents directly. As such, not withstanding any other provision in the Agreement to the contrary, the District shall not be responsible under the terms of this Agreement to collect consent from individual parents.

8. **Federal Work Authorization Program.** Prior to commencement of any work contemplated under this Agreement, Company shall provide to the District a sworn affidavit and other sufficient documentation to affirm its enrollment and participation in the Federal Work Authorization Program. Federal Work Authorization Program means the eVerify program maintained and operated by the United States Department of Homeland Security and the Social Security Administration, or any successor program. Company shall also provide the District a sworn affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services.

9. **Background Checks**Before employment of any employee, contractor, subcontractor, consultant or subconsultant who is an individual for work on the services set forth in this Agreement, the Company shall conduct or shall allow the District to conduct background checks through all appropriate state agencies and any other background checks as may be standard for entities providing services to public schools, including without limitation, a thorough review of the list of registered sex offenders as provided by the County Sheriff's Department, the Federal Bureau of Investigation's criminal history files, the Missouri Highway Patrol's criminal history database and sexual offender registry, the Family Care Safety Registry, or the central registry of child abuse and neglect of the Missouri Children's Division; and any such individual who does not pass such background check as determined by the District in its sole discretion shall not be permitted to enter the premises where the services are being performed or any other school district property or to work on the services under this Agreement. The Company shall include all of these requirements in its contracts with their subcontractors and suppliers.

10. **Drugs and Alcohol.** The Company shall be responsible to the District for acts and omissions of the Company's employees, subcontractors and their agents and employees, and other persons or entities performing portions any work contemplated under this Agreement for, or on behalf of, the Company or any of its subcontractors. As part of that responsibility, Company shall enforce the District's alcohol-free, drug-free, tobacco-free, harassment-free and weapon-free policies and zones, which will require compliance with those policies and zones by Company's employees, subcontractors, and all other persons carrying out the Agreement.

11. INTENTIONALLY OMITTED

12. **Governing Law.** This Agreement will be construed and enforced in accordance with

Missouri law.

13. **Forbearance.** The failure or delay of the parties to insist on the timely performance of any of the terms of this Agreement, or the waiver of any particular breach of any of the terms of this Agreement, at any time, will not be construed as a continuing waiver of those terms or any subsequent breach, and all terms will continue and remain in full force and effect as if no forbearance or waiver had occurred.

14. **Immunity**. No provision of this agreement shall be construed in such a way as to waive or terminate the statutory or common law immunities enjoyed by District. District shall retain all immunities, including those immunities contained within Missouri Revised Statute § 537.600 et.seq.

15. **Assignment**. This Agreement cannot be assigned by either party without the prior written consent of the other party.

16. **Entire Agreement**. This Agreement, including the Data Governance Addendum (Exhibit A), is the entire Agreement between Company and District and supersedes any prior oral understandings, written agreements, proposals, or other communications between Company and District. Company's standard Terms of Service and Privacy Policy shall not apply to this Master Terms or current or future Sales Contracts.

17. **Modification**. Any change or modification to this Agreement will not be effective unless made in writing. This written instrument must specifically indicate that it is an amendment, change, or modification to this Agreement.

18. **Binding Effect.** The obligations, covenants, terms, conditions, provisions, and undertakings in this Agreement, or in any amendment, will be binding upon the parties' heirs, successors, and permitted assigns.

19. **Severability.** If any court of competent jurisdiction finds any provision or part of this Agreement is invalid, illegal, or unenforceable, that portion will be deemed severed from this Agreement, and all remaining provisions and parts of this Agreement will remain binding and enforceable; the parties will reconvene negotiations to arrive, in good faith, at an agreement as to matters remaining undetermined as a result of any finding by a court of competent jurisdiction that any provision or part of this Agreement is invalid, illegal, or unenforceable.

Company	*Raytown Quality Schools*
By: Jim Bowler *Name: Jim Bowler* *Title: CEO* *Date: 6/20/22*	*By:* [signature] *Name:* Chris Grenier *Title:* Chief Academic Officer *Date:* 7/7/22

EXHIBIT A

Data Governance Addendum for District Data of the Raytown C-2 School District

Definitions.

- **FERPA**: means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1), as amended from time to time.
- **Security Breach (Security Incident)**: means actual evidence of a confirmed unauthorized acquisition of, access to, or unauthorized use of any Student Education Record(s), Personally Identifiable Information, User Data or other district confidential information.
- **Personally Identifiable Information (PII)**: includes but is not limited to (a) student's name; (b) name of the student's parent or other family members; (c) address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; and (e) other indirect personal identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) 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 (g) "medical information" as may be defined in state law; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; (h) nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; (i) 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; (j) other financial account numbers, access codes, driver's license numbers; (k) and state- or federal-identification numbers such as passport, visa or state identity card numbers; (l) personal identifiable information as defined by COPPA, including but not limited to online contact information like an email address or other identifier that permits someone to contact a person directly (for example, an IM identifier, VoIP identifier, or video chat identifier), screen name or user name where it functions as online contact information, telephone number, persistent identifier that can be used to recognize a user over time and across different sites (including a cookie number, an IP address, a processor or device serial number, or a unique device identifier), a photo, video, or audio file containing a child's image or voice, geolocation information sufficient to identify a street name and city or town; or other information about the child or parent that is collected from the child and is combined with one of these identifiers.
- **Student Education Record**: means identifiable information, including but not limited to PII, of Subscriber's students that may be considered part of an educational record as defined by FERPA, district policy, and any applicable state law.
- **Anonymized Data**: means any Student Education Record rendered anonymous in such a manner that the student is no longer identifiable. For example, this includes non-identifiable student assessment data and results, and other metadata, testing response

times, scores (e.g. goals, RIT), NCES codes, responses, item parameters, and item sequences that result from the Services.

- **De-identified Data (Pseudonymized Data)**: means a Student Education Record processed in a manner in which the Student Education Record can no longer be attributed to a specific student without the use of additional information, provided that such additional information is kept separately using technical and organizational measures. Attributions may include, but are not limited to: name, ID numbers, date of birth, demographic information, location information, and/or any other unique metadata.
- **User Data**: any data provided by the District or collected from the District or authorized users, PII, metadata, user content and/or any data part of a student education record that is not anonymized or de-identified.

Conditions. Terms used herein shall have the same meaning as in the Master Terms unless otherwise specifically provided. To the extent that 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 the Master Terms, Terms of Service or Privacy Policy conflict with or contradict with this addendum, in letter or spirit, the provisions of this addendum shall prevail.

Designation: Raytown Quality Schools hereby designates ESGI, LLC as a "School Official" with "legitimate educational interests" in the District's records, as those terms have been defined under FERPA and its implementing regulations, and Company agrees to abide by the FERPA limitations and requirements imposed upon School Officials. Company and District acknowledge that Company will create, access, secure, and maintain Student Education Records to perform the Services as further outlined in Master Terms and/or Sales Contract. Company shall not resell Student Education Records or use Student Education Records for targeted student advertising or disclose to third parties any Student Education Records without the written consent of District. District grants permission to Company and its contractors that have executed confidentiality agreements to use Student Education Records for maintaining and providing the Services.

Compliance with Federal and State Confidentiality and Privacy Laws: Company and the District agree and understand that this Agreement must be in compliance with all federal and state confidentiality and privacy laws which includes, but is not limited to: the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); Protection of Pupil Rights Amendment ("PPRA") (20 U.S.C. § 1232h; 34 CFR Part 98), all of them which may be in effect or amended from time to time, including any successor statute and its implementing regulations and rules. In the event of a conflict between this Agreement and the Confidentiality Laws, the Confidentiality Laws shall control. In the event of a conflict between FERPA and all other Confidentiality Laws, FERPA will control absent clear statutory authority on controlling law.

- Company shall be responsible for the timing, content, and costs of such legally-

required notifications that arise as a result of Company's failure to comply with its obligations as a Service Provider under COPPA, FERPA or other applicable laws. Furthermore, Company shall be responsible for the cost of investigating the above non-compliance, as well as the payment of actual, documented costs including reasonable legal fees, audit costs, fines, and other fees imposed against the District as a result of the non-compliance.

Data Governance:

Limited Collection, Disclosure, Access and Use:

- Confidentiality: Company and its officers, employees, and agents agrees to hold district data in strict confidence and use the data only for the limited purpose outlined in the Master Terms and/or Sales Contract.

- Non-Disclosure: Company affirms that its services will be conducted in a manner that does not disclose Customer data to anyone who is not an authorized representative of the Company.

- Data Collection: Company will only collect data necessary to fulfill its duties as outline in this Agreement.

- Data Use: Company will use data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement. The approval to use District data for one purpose does not confer approval to use the data for another or different purpose.

- Access Records: Company will keep true and complete records of any and all data received, exchanged and shared between and amongst its employees, agents, subcontractors and volunteers.

- Sub-processors (Contractors and Agents): Company shall enter into written agreements with all Sub-processors performing functions pursuant to this Agreement, whereby the Sub-processors agree to protect District User Data in a manner consistent with the terms of this Agreement.

- De-Identified Data: De-identified information may be used by the Company for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public would be able to use de-identified data. The Company and District agree that the Company cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Company agrees not to attempt to re-identify de-identified User Data and not to transfer de-identified User Data to any party unless (a) that party agrees in writing not to attempt re-identification, (b) Company can guarantee that the party has not been provided any other de-identified information, that in combination with other provided information can be used to re-identify User Data and (c) prior written notice has been given to the District

who has provided prior written consent for such transfer.

- Company Access to District Data. The parties agree that Company shall exclusively limit its employees, contractors, and agents' access to and use of District data to those individuals who have a legitimate need to access District data in order to provide required support of the system or services to the District 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, including background checks, to ensure that such individuals have no significant criminal history.

    - Employee Obligation: Company shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this Agreement. Company agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to District Data.

    - Employee Training: Company shall provide periodic security training to those of its employees who operate or have access to the system.

Data Storage/Maintenance. The parties agree that all data collected or held by Company (including but not limited to District students' names and other information) shall be stored within the United States of America. No data may be stored or backed up outside of the continental United States.

Data Security: Company shall maintain and process all data in a secure manner using industry best practices regarding technical, physical, and administrative safeguards. Company utilize appropriate administrative, physical and technical safeguards to secure data from unauthorized access, disclosure, and use. Company will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

Data Encryption. In conducting data transactions and transfers with the District, 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 industry best practices in administrative, physical and technical safeguards designed to secure User Data and District 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 District provided Company or that Company collected from District or its authorized users, ("Security Incident"), then Company will promptly (within five (5) business days), 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 District and will use reasonable efforts to cooperate with the District'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 District's investigation and third-party notifications, if any, at the District's direction and expense.

- Company shall be responsible for the cost of investigating any Security Incident determined to be caused by the acts or omissions of Company or its agents, employees, or contractors, as well as the payment of actual, documented costs including reasonable legal fees, audit costs, fines, and other fees imposed against the District as a result of a Security Incident.

- Company shall also be required to outline for the District 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.

- Company further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of User Data or any portion thereof, including personally identifiable information and agrees to provide Customer, upon request, with a copy of said written incident response plan.

Cyber Security Insurance. Company will provide to the District a certificate of insurance including Cyber Security Insurance coverage for Data Breach.

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

Data Ownership. The parties agree that, notwithstanding Company's possession of or physical control over District data, the District maintains ownership and control of all data that the District provides to Company or that Company collects from the District and/or authorized users. Company further agrees that District 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 District in writing.

- Parent Access: District has established procedures by which a parent, legal guardian, or eligible student may review education records and correct erroneous information. Company shall cooperate and respond within ten (10) days to the District's request for User Data and/or Education Records held by Company to view or correct as necessary. In the event that a parent or other individual contacts the Company to review any User Data, Company shall refer the parent or individual to the District, who will follow the necessary and proper procedures regarding the requested information.

- Third Party Access: Should a Third Party, including, but not limited to law enforcement, former employees of the District, current employees of the District, and government

entities, contact Company with a request for data held by the Company pursuant to the Services, the Company shall redirect the Third Party to request the data directly from the District and shall cooperate with the District to collect the required information. Company shall notify the District in advance of a compelled disclosure to a Third Party, unless legally prohibited.

Data Handling in the Event of Termination. In the event that the parties terminated their agreement for the provision of Company's services, upon written request any District data within Company's possession or control must be provided to the District 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 to transfer de-identified data to any party unless that party agrees not to attempt re-identification. If District data is disclosed without de-identifying the same as required herein, written notice shall be provided to the District. If District 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.

Company Visits to District Property. The parties recognize that certain Company employees, contractors, or agents may visit the District's property in order to obtain the necessary information for the provision of Company's services. In the event that a Company employee must be unsupervised on District's property, the parties agree that, before any such visits to the District 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 District will not have contact or interact with the District's students. Company will indemnify, defend, and hold the District, 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 District's property as described herein.