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

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

- Data Storage/Maintenance. The parties agree that all data collected or held by Company (including but not limited to Raytown Quality Schools "Customer" 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, 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 Customer as a result of a Security Incident. Company shall also be required to outline for 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 Dictionary. 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 Customer data pertaining to personally identifiable information.

- 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 provision 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 to 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 Data Breach.

- Company Visits to Customer Property. The parties recognize that certain Company employees, 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 event 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.

Raytown Quality Schools

Signature

Melissa Tebbenkamp

Typed or Printed Name

Director of Instructional Technology

Title

2/26/18

Date

EdClub, Inc.

Signature

Ramtin Kiany

Typed or Printed Name

President

Title

3/1/2018

Date