EVERFI

MOU AND PRIVACY POLICY

EVERFI, Inc. and the School District

Memorandum of Understanding

This MEMORANDUM OF UNDERSTANDING (the "*Agreement*") is made and entered into as of the 1st day of July, 2018 (the "*Effective Date*"), by and between EVERFI, Inc. ("EVERFI") and the Raytown School District, on behalf of itself and each of its participating schools (collectively, "District"). For purposes of this Agreement, EVERFI and the District shall be referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, EVERFI is a leading education technology company with the mission to help Districts teach critical topics such as financial capability, character education, career choice and digital literacy; and

WHEREAS, the District wants to empower students to succeed in school, college, careers and life and believes that EVERFI's digital curriculum will help teachers provide engaging, high quality, and consistent instruction to do so; and

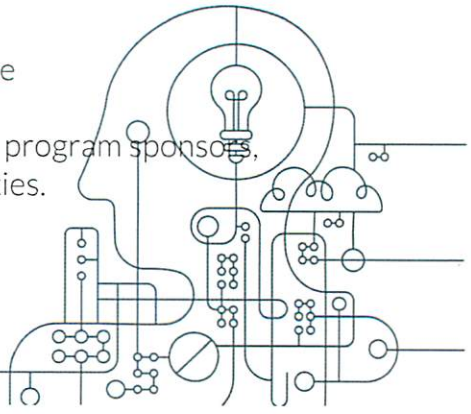
WHEREAS, EVERFI and the District desire to create an agreement to bring EVERFI curriculum to schools within the District.

NOW, THEREFORE, for good consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties, intending to be legally bound, agree as follows:

Responsibilities of EVERFI:

EVERFI shall:

- Provide EVERFI's sponsored digital curriculum to schools within the District at no cost. This curriculum will be available the entire school year and in the summer, and the specific resources and objectives can be found at www.EVERFI.com/k12.
- Provide free professional development (PD) for teachers. EVERFI can deliver PD on an individual teacher/school basis or large group basis. Large group PD's are preferred.
- Provide real-time data for teachers on student progress via a digital teacher dashboard.
- Provide 24/7 support to teachers regarding implementation or technical questions related to its digital curriculum.
- Provide an annual Impact Report to the District highlighting the impact of the curriculum.
- Provide opportunities for schools, as available, to interact with program sponsors, including special events, classroom visits, and other opportunities.



- Include District teachers and administrators in webinars and other events hosted by EVERFI about life skills for students.
- Provide the District with marketing materials to promote the program and its impact, including press releases, social media guides, and more.
- Meet high standards for student data privacy – EVERFI's K12 policy is outlined in Exhibit A.
- Provide the District with an EVERFI point of contact for the program and for any contract related questions.
- Provide access to EVERFI's curriculum through the District's SSO provider.

Responsibilities of the District:

The District shall:

- Identify an overall point person for EVERFI to coordinate an annual meeting and other partnership details.
- Identify additional points of contact, for each subject area, who can help determine the appropriate placement for EVERFI sponsored learning courses. The placement of the courses will aim to reach the most students and achieve the best student outcomes.
- Invite EVERFI staff to present at relevant teacher PD's throughout the school year or help set up other means of training teachers.
- Meet with EVERFI staff annually over the summer to review the results of the annual Impact Report and to discuss the partnership for the following school year.
- Complete an annual survey providing feedback to EVERFI staff about the partnership.
- As District deems appropriate, share elements of the partnership via social media and other outlets or provide a thank you or recognition to the sponsors funding EVERFI's programs.
- Ensure that EVERFI has teacher and student SIS information for all relevant grades and subject areas prior to the beginning of each school year. This information will be used by EVERFI to provide teachers and students access to the EVERFI curriculum through the district's single-sign-on. See exhibit B for EVERFI's full K12 data sharing agreement.

Term:

This Agreement is for the entire school year and will renew automatically each year on July 1st for the upcoming and academic year unless EVERFI or the District give one month notice of termination. Both EVERFI and the District also reserve the right to terminate this Agreement upon thirty (30) days prior written notice if the other Party fails to perform the terms and conditions in this Agreement.

Mutual Protections:

This Agreement shall be interpreted and governed by the laws of the District of Columbia excluding any laws that direct the application of another jurisdiction's law.

Except as required by law, neither Party shall be liable to the other for consequential, special, punitive, incidental or indirect damages whether arising in contract, in tort or otherwise in connection with performance or failure to perform the Agreement.

In the event that any provision or provisions of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall continue in full force and effect.

Any modification or assignment of the Agreement will be effective only if in writing and signed by both parties. A waiver of any term or condition of this Agreement must be in writing executed by both parties.

Any notices to be given under this Agreement by either party to the other may be effected by personal delivery in writing or by mail, registered or certified, postage prepaid with return receipt requested.

This Agreement may be executed in any number of counterparts.

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the date and year first above written.

EVERFI, INC.	DISTRICT (~~School District~~)
Signed: _____	Signed: _____
Print: Timothy Convey	Print: Brian Huff
Title: Vice President, K12	Title: Associate Sup C&I
Date: 1.10.19	Date: 1/7/19

EVERFI

EXHIBIT A

EVERFI K12 Data Privacy Policy

Overview

As a provider of online content, EVERFI takes student privacy very seriously and complies with two specific pieces of legislation protecting student privacy:

- Family Education Rights and Privacy Act (FERPA): Mandated by the Department of Education to protect the privacy of education records while still allowing for effective use of data.
- Children's Online Privacy Protection Act (COPPA): Mandated by the FTC to protect children under 13 from unfair or deceptive uses of personal information.

Both of these regulations address third party handling of Personally Identifiable Information (PII) and Education Records. EVERFI collects a narrow set of PII, referred to as "Directory Information" under FERPA. Schools have the right to share this information with EVERFI, and EVERFI has the right to store this information so long as the information is not disclosed to third parties, and there are proper measures in place to delete all records upon request.

As a practice, EVERFI only uses PII for core business practices such as troubleshooting technical issues and presenting teachers with reports for individual students (such as rosters and scores). All student data, when analyzed internally or shared externally, is aggregated and de-identified, meaning it cannot be traced back to individual students.

If a student is enrolled in the EVERFI digital curriculum under the FERPA School's Official Exception and a parent requests deletion of such student's student record, EVERFI shall direct such request to the student's school.

Nothing contained herein shall prohibit EVERFI from complying with applicable law.

PII Related Data Being Stored (K-12)

- Date of Birth is requested (to support COPPA compliance) but is only stored as an over/under 13 flag.
- If a student is flagged as over 13, email is optional and first name and last name are required.
- If a student is flagged as under 13, email is not collected and first name and first initial of last name (1 character only) is required for the sole purpose of helping teachers identify students. As an alternative, teachers can direct students to register with ID numbers instead of names.

General Privacy Policy and Data Security

EVERFI DOES NOT:

- Use student data to create student profiles or perform any other type of data mining that might result in damaging or discriminatory representations of student ability
- Use or sell student data for commercial purposes, such as creating targeted ads
- Use or sell student data for marketing research purposes
- Share email addresses or individual student data with third parties
- Store PII data on removable drives
- Email PII data directly to anyone

EVERFI DOES:

- Analyze and report on student data in de-identifiable and/or aggregate form, either to improve our learning products or communicate the impact of a program to third parties. Data is retained only for educational purposes.
- Use best of breed cloud-based hosting and system admin services in Amazon Web Services to host and keep all data secure
- Encrypt all data at rest, encrypt all hard-drives, and use TLS encryption for data transfer
- Use role-based access control on a need-to-know basis for staff
- Incorporate appropriate password policies based on specific roles and markets
- Archive and remove student data every 4 years (on a rolling basis)
- Run vulnerability and penetration security testing
- Have formal policies and programs in place regarding:
    - System Change Management
    - Staff Security Training and Review
    - System Log Monitoring, Review, and Audit
    - User Access Monitoring, Review, and Audit
    - Service Interruption Contingency and Support Escalation

EXHIBIT B

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 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 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.

- 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.