

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

WHEREAS, the Allegany County Public Schools (hereinafter ACPS) desires to utilize services provided by vendor and vendor has agreed to provide services to ACPS and its students and/or staff; and

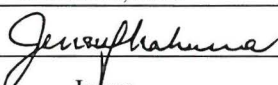
WHEREAS, in order to perform the services requested the vendor will need access to ACPS student data and/or staff data; and

WHEREAS, some of said data is directory information and some of said data includes personally identifiable information which is confidential information as defined under the Federal Family Education Rights Act ("FERPA") and the Health Insurance Portability and Accountability Act ("HIPPA"). Confidential information is subject to the provisions of Md. Education Code Ann. § 4-131 and may include but is not limited to: login, password, last name, first name, email address, and grade level.

NOW, THEREFORE, the parties do hereby agree as follows:

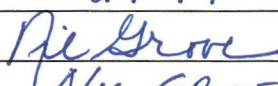
1. ACPS shall furnish to vendor information which may include confidential information as described in the recitals above and may further allow vendor the right to discuss or interview representatives of the ACPS with regard to that information. ACPS will determine the method and manner to distribute the information.
2. Vendor agrees that it will hold confidential information in trust and confidence and that it will obtain, maintain, use, transmit, and release any and all student and/or staff records during the term of the agreement and thereafter only in accordance with both "FERPA" and "HIPPA" privacy and security safeguards. Vendor further agrees that the information shall be used only for the contemplated purposes, shall not be used for any other purpose, or disclosed to any third party.
3. Except for electronic copies made for archival, backup or disaster recovery purposes, no copies will be made or retained of any information or prototypes supplied without the permission of ACPS.
4. All confidential information in whatever format, including prototypes, written notes, photographs, sketches, models, memoranda or notes taken shall be returned to ACPS at the conclusion of the project being performed for ACPS or upon demand by ACPS. At vendor's discretion, such information may be destroyed by vendor with such destruction certified in writing to ACPS.
5. Confidential information shall not be disclosed to any employee, consultant or third party unless they agree to be bound by the terms of this Agreement, and have been approved by ACPS.
6. Vendor must immediately notify ACPS if they are aware of a breach or unauthorized access to student or employee confidential data. Vendor will take such steps as directed by ACPS to mitigate damages resulting from such breach.
7. The recitals described above are considered fundamental parts of this agreement.
8. This Agreement shall be governed by the laws of the State of Maryland.

AGREED AND ACCEPTED BY:

Vendor EVERFI, Inc.
Date March 26, 2019
Signature 
Printed Name Jenny
Nakamura
Title K12 Regional Director

Witness: _____

Allegany County Board Of Education

Date 3-29-19
Signature 
Printed Name NIC GROVE
Title CIO

Witness: 

May 24, 2016

File w/NDAs
- waiting on
spread form
3-15-19

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.

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