

# CALIFORNIA AB 1584 COMPLIANCE STATEMENT

Updated: September 30, 2019

This Statement describes the policies and procedures employed by Educa to ensure compliance with the requirements set forth in Section 49073.1 of the California Education Code (the “Code”). For the purposes of this Statement, “System” shall mean the bundle of services provided Educa via its website and/or mobile application, and “Authorized User” shall mean any employee of a School District that is authorized to access and utilize the System in connection with such employment.

**Ownership of Pupil Records:** Any and all Pupil Records provided to Educa, or to which Educa has been granted access, are and shall remain the sole property of the School District or educational agency (collectively, “School District”) that provided or granted access to such records.

**Pupil-Generated Content:** The default setting in the Educa System is that it does not collect or store any Pupil- Generated content. However, there is a feature where pupils are given user access and can create content. This content is owned by the School District or educational agency. However, pupils also have the absolute right to access and download their content.

**Third Party Access and Use:** Educa prohibits all third parties from accessing or utilizing any Pupil Record for any purpose other than those required by or permitted by the contract for Educa’s services.

**Parent and Pupil Review Procedures:** The System enables any Authorized User to permit parents, legal guardians, and eligible pupils to review personally identifiable information contained in Pupil Records, and to correct erroneous information, in accordance with procedures established by the School District.

**Security and Confidentiality of Pupil Records:** Educa is committed to maintaining the security and confidentiality of Pupil Records. It has designated a Security Compliance Officer (SCO), who is responsible for:

(a) ensuring that Educa servers are protected against unauthorized access to the greatest degree possible; (b) limiting employee access to Pupil Records to whatever extent is required for them to perform their job functions; and (c) training employees in data security procedures to further ensure compliance with company data security policies.

**Unauthorized Disclosure:** In the event any Pupil Records are inadvertently disclosed via outside data breach or for any other reason, the SCO shall notify the School District that owns such records immediately upon the discovery of such inadvertent disclosure. The School District may in turn utilize the System to notify affected parents, legal guardians, or eligible pupils via posts within the System, emails, or in such other manner as the School District deems appropriate.

**Post-Contract Data Deletion:** Educa hereby certifies that, upon the termination of a service contract with a School District, it shall isolate and permanently delete any and all Pupil Records belonging to such School District that may remain on the System, unless the School District or applicable regulations require the retention of such data, in which case the records shall be deleted upon the expiration of the retention period. Prior to deleting any Data Records, Educa shall first ensure that the School District has downloaded backups of the same.

**FERPA Compliance:** Educa offers School Districts utilizing the System the means to comply with their obligations under the Federal Educational Rights and Privacy Act (20 USC §1232(g)), by enabling Authorized Users to inspect and review Pupil Records and to correct any inaccuracies therein as described in Section 4 of this Statement.

**Prohibition Against Targeted Advertising:** Educa strictly prohibits the use of any personally identifiable information included in a Pupil Record to direct targeted advertising for any product or service. In furtherance of this prohibition, Educa does not sell, trade, or rent any element of personally identifiable information to any third party.

Additional privacy information is included in the Educa online Privacy Policy.