

EXHIBIT A: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

E2CCB is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, E2CCB wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be submitted to NYSED at www.nysed.gov/data-privacy-security; by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

Supplemental Information to Parents Bill or Rights for Data Privacy and Security:

1. The exclusive purpose for which Agile Sports Technologies, Inc., d/b/a Hudl (hereinafter "Contractor") is being provided student data and/or teacher or principal data, and for which such information will be used, is to provide the products and services for which E2CCB has contracted. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from E2CCB or its employees, officers, agents, and/or students will not be sold or used for commercial purpose or marketing purpose.
2. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, all of Contractor's employees are provided such training upon commencing employment and as necessary thereafter. Any subcontractors engaged by Contractor, and which have access to student data and/or teacher or principal data, are required to execute legally binding agreements with Contractors acknowledging the subcontractor's obligation to comply with data security and privacy standards at least as restrictive as those required of Contractor under the Data Privacy and Security Agreement between E2CCB and Hudl, as well as applicable state and federal law.

3. The agreement between Contractor and E2CCB for products and/or services expires on July 31, 2022. At the expiration of that agreement without a successor agreement in place, Contractor will either maintain any and all student data and/or teacher or principal data in its possession in accordance with the terms of this Agreement or assist E2CCB and/or the educational agency from which the data originated in transferring such data back to requesting educational agency. Additionally, upon request, Contractor will securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the deletion or destruction of student data and/or teacher or principal data will be completed within 30 days of the request and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to E2CCB from an appropriate officer that the requirements of this paragraph have been satisfied in full.

4. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the E2CCB for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the BOCES Annual Professional Performance Review Plan.


5. Student data and/or teacher or principal data transferred to Contractor by E2CCB or E2CCB officers, employees, agents, or students will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection. More specifically, Contractor has implemented the following administrative, operational, and technical safeguards:

- a. Prospective employees are subject to extensive screening, testing, interviews, and referral checking.
- b. All personnel, including third parties, are subject to strict confidentiality

agreements which form part of the contracts that are signed when they work for or with Contractor.

- c. Physical access to Contractor's offices requires individually assigned secure door-entry badges, with staffed reception desks and video surveillance cameras in use.
 - d. For the purpose of data storage, Contractor utilizes Amazon Web Services, which has certification for compliance with ISO 27001, 27017, and 27018.
 - e. Contractor utilizes malware protection systems in multiple locations, including within email message flows and on workstations.
 - f. Contractor employs email content security solutions and other application aware systems to help protect against data leakage.
 - g. Firewalls and virtual private networks help secure access to Contractor's systems, with more sensitive data placed in logical silos.
 - h. All Contractor's systems send logs to a single central analysis center for monitoring and review.
6. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest.

Acknowledged and agreed to by:

Signature: 

Name: McKenzie Swanson

Title: Manager, Competitive Sales

Date: 09/14/2021