

EXHIBIT A - Education Law § 2-d Parents' Bill of Rights for Data Privacy and Security

NORTH COLLINS CENTRAL SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY Summary of Rights and Information for Parents and Students

The North Collins Central School District is committed to ensuring the privacy of student personally identifiable information and recognizes that parents (including legal guardians or persons in parental relationships) and eligible students (students 18 years of age and older) are entitled to certain rights with regard to a student's personally identifiable information. To this end, the District is providing the following Parent's Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information ("PII") cannot be sold or released for any commercial purposes. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR § 99.3 for a more complete definition.
2. Parents and/or eligible students have the right to inspect and review the complete contents of the student's education records stored or maintained by the District. This right may not apply to parents of an eligible student.
3. State and federal laws such as New York Education Law § 2-d, the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA, the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and the Individuals with Disabilities Education Act protect the confidentiality of a student's PII.
4. 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.
5. A complete list of all student data elements collected by the State is available for public review at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. Parents have the right to have complaints about possible breaches and unauthorized disclosures of PII addressed.

- a. Complaints should be submitted to the District at: Brian Zolnowski Director of Information Technology and Communications Services North Collins Central School District 2045 School St, North Collins, NY 14111 Email: bzolnowski@northcollinscsd.org, 716-337-0101 x1100.
 - b. Complaints may also be submitted to the New York State Education Department at: www.nysed.gov/data-privacy-security/report-improper-disclosure or by contacting the State’s Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, privacy@nysed.gov, 518-474-0937.
7. District contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements and will include supplemental information that provides:
- a. The exclusive purposes for which student data or teacher or principal data will be used;
 - b. How the third party contractor will ensure that the subcontractors, persons or entities that the vendor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
 - c. When the agreement expires and what happens to student data or teacher or principal data upon expiration of the agreement;
 - d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
 - e. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including how such data will be encrypted.
8. Parents and/or eligible students have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
9. District workers who handle PII will receive annual training on applicable federal and State laws, regulations, policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

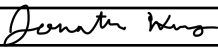
WeVideo, Inc.	
By: (Signature)	
(Printed Name)	Jonathan Huang
(Title)	Deputy DPO
Date:	5/12/21

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors (“Service Agreements”) that will receive Personally Identifiable Information (“PII”) from Student Data or Teacher or Principal APPR Data.

WeVideo, Inc.	
Term of Service Agreement	Agreement Start Date: 5/12/2021 Agreement End Date: 5/12/2022
Description of the purpose(s) for which Contractor will receive/access/use PII	PII received by the Contractor will be received, accessed and used only to perform the Contractor’s Services pursuant to the Service Agreement with the District. List Purposes: WeVideo for Schools, a collaborative online video recording/editing/creating/sharing platform
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> Teacher or Principal APPR Data
Subcontractor Written Agreement Requirement	The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Service Agreement. Check applicable option. <input type="checkbox"/> Contractor will not utilize Subcontractors. <input checked="" type="checkbox"/> Contractor will utilize Subcontractors.

<p>Data Transition and Secure Destruction</p>	<p>Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing:</p> <ul style="list-style-type: none"> • Securely transfer data to District, or a successor contractor at the District’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
<p>Challenges to Data Accuracy</p>	<p>Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District’s written request.</p>
<p>Secure Storage and Data Security</p>	<p>The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.</p> <p>Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data:</p> <p>(a) Storage of Electronic Data (check all that apply):</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other: <p>(b) Storage of Non-Electronic Data:</p> <p>Secured file cabinets, 24/7 keycard access, office security</p>

	<p>(c) Personnel/Workforce Security Measures: Background checks on employees At minimum, annual cybersecurity awareness training Privacy Pledge</p> <p>(d) Account Management and Access Control: Minimal required access granted, IAM management (AWS), 2fa requirements, strong password policy</p> <p>(e) Physical Security Measures: Devices encrypted, endpoint protection (ESET), keycard access</p> <p>(f) Other Security Measures:</p>
Encryption	Data will be encrypted while in motion and at rest.

WeVideo, Inc.
By: (Signature) <i>Jonathan Huang</i>
(Printed Name) Jonathan Huang
(Title) Deputy DPO
Date: 5/12/21