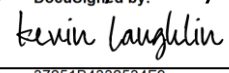


PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Fillmore CSD is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, Fillmore CSD informs the school 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 New York State is available for public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to Fillmore CSD Data Privacy Officer, 104 W. Main St, Fillmore, New York 14760 or by using the form available at the following website: <https://www.fillmorecsd.org/Page/2923>. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first written above.

DocuSigned by:

3725164332534F9
Authorized Vendor Signature

2020-08-17

Date

Kevin Laughlin

CFO

Michael Dodge

Authorized Fillmore CSD Signature

8/18/2020

Date

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: <u>Clever</u>		Product: <u>Rostering, SSO</u>	
Collects	<input type="checkbox"/>	X Student Data	X Teacher or Principal Data
:	<input type="checkbox"/>		<input type="checkbox"/> Does not collect either

Educational agencies including Fillmore Central School District are required to *post information about [third-party contracts](#) on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to [NYS Education Law 2-d](#) and [Part 121.3 of the Commissioner's Regulations](#). Note that this applies to all software applications and to mobile applications ("apps"). All capitalized or lower case terms used herein and defined in the Data Sharing and Confidentiality Agreement to which this is attached shall have the meanings given to them in such Data Sharing and Confidentiality Agreement.

Parents' Bill of Rights for Data Privacy and Security: Supplemental Information

Third Party Contractor: Clever, Inc.(the "third-party contractor")
Educational Agency: (the "District")

New York Education Law §2-d requires educational agencies to make a Parents' Bill of Rights for Data Privacy and Security available to the public, along with additional information concerning agreements with third party contractors under which personally identifiable student information and certain teacher and principal information (referred to herein as "student data or teacher or principal data") is disclosed. In accordance with these provisions, it is necessary for Recipient to provide the following information to the District.

(1) *The exclusive purposes for which the student data or teacher or principal data will be used:* The student data or teacher or principal data received by the third-party contractor will be used only to perform the third-party contractor's obligations pursuant to its agreement with the District and for no other purpose.

(2) *How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including those outlined in applicable state and federal laws and regulations:* The third-party contractor limits access to student data or teacher or principal data only to those employees or trusted service providers who have a legitimate need to access such data in the performance of their duties or in connection with providing services to the District. Of course, anyone involved in the handling of student data or teacher or principal data will treat such data as strictly confidential and shall not redisclose such data except as necessary in order to provide services to the District. The third-party contractor will maintain access log(s) that record all disclosures of or access to student data or teacher or principal data within its possession and will provide copies of those access log(s) to the

District upon request. In addition, the third-party contractor provides employee training on privacy and data security laws and best practices. If there is any disclosure of or access to any student data or teacher or principal data by an unauthorized party, the third-party contractor will promptly notify any affected schools and will use reasonable efforts to cooperate with their investigations of the incident.

(3) The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement: The agreement with the District expires when terminated in accordance with its terms. Upon the termination of the third-party contractor's agreement with the District for any reason, the third-party contractor will, as directed by the District in writing, securely destroy ("securely destroy" means taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means) or return all student data or teacher or principal data received by the third-party contractor as soon as reasonably possible.

(4) 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: The third-party contractor will work with the District in processing challenges to the accuracy of student data or teacher or principal data in the custody of the third-party contractor.

(5) Where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated: The third-party contractor stores its data in the United States and takes strong measures to keep data safe and secure. The third-party contractor maintains strict administrative, technical and physical procedures to protect information stored in its servers. Access to information is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. The third-party contractor uses industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include, but are not limited to, data encryption, firewalls, and physical access controls to buildings and files. The third-party contractor uses bank-grade security infrastructure at the software and network level, to ensure that student records are always encrypted and transmitted securely. This includes use of TLS / SSL protocols, API call level authentication, and API bearer tokens with 200 bits of entropy. The third-party contractor's Transport Layer Security requires that all data transferred via its website and API use the Transport Layer Security (TLS) cryptographic protocol over a HTTPS connection. This means that unique session keys are used to encrypt and decrypt data transmissions and to validate transmission integrity. The third-party contractor's servers prefer perfect forward secrecy (using ECDHE) to encrypt data using 256 bit Advanced Encryption Standard (AES) – which surpasses the standard adopted by the consumer banking industry and the U.S. Government for the secure transmission of classified data. The third-party contractor limits access to student data or teacher or principal data only to those employees or trusted service providers who have a legitimate need to access such data in the performance of their duties or in connection with providing services to the District under its agreement with the third-party contractor. Anyone involved in the handling of student data or teacher or principal data will treat such data as strictly confidential and shall not redisclose such data except as necessary in order to provide services to the District. As discussed

above, the third-party contractor will maintain access log(s) that record all disclosures of or access to student data or teacher or principal data within its possession and will provide copies of those access log(s) to the District upon request. In addition, the third-party contractor provides employee training on privacy and data security laws and best practices. If there is any disclosure or access to any student data or teacher or principal data by an unauthorized party, the third-party contractor will promptly notify any affected schools and will use reasonable efforts to cooperate with their investigations of the incident.

(6) Address how the data will be protected using encryption while in motion and at rest:

The third-party contractor encrypts all student data or teacher or principal data in transit outside of its private network and at rest in its private network. The third-party contractor uses strong forms of cryptography like AES256-GCM with access-controlled keys that are regularly audited and rotated. The third-party contractor's TLS configuration gets an A+ from ssllabs.com, and it uses HSTS to ensure that pages are loaded over HTTPS connections.