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

Third Party Contractor: Clever, Inc.(the "Recipient)
Educational Agency: Ichabod Crane Central Schools (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 (collectively "PII") is disclosed. In accordance with these provisions, it is necessary for Recipient to provide the following. If an item is not applicable to Recipient's agreement with the District, please explain why.

(1) The exclusive purposes for which PII will be used: The PII received by the Recipient will be used only to perform the Recipient's obligations pursuant to its agreement with the District and for no other purpose.

(2) How you Recipient ensure that the subcontractors or other authorized persons or entities that Recipient will share the PII with, if any, will abide by data protection and security requirements: The Recipient limits access to PII 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 PII 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 Recipient will maintain access log(s) that record all disclosures of or access to PII within its possession and will provide copies of those access log(s) to the District upon request. In addition, the Recipient provides employee training on privacy and data security laws and best practices. If there is any disclosure of or access to any PII by an unauthorized party, the Recipient will promptly notify any affected schools and will use reasonable efforts to cooperate with their investigations of the incident.

(3) *When the agreement with the District expires and what happens to PII upon expiration of the agreement:* The agreement with the District terminates as provided for therein. Upon the termination of the Recipient's agreement with the District for any reason, the Recipient 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 PII received by the Recipient as soon as reasonably possible.

(4) If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the PII that is collected: The Recipient will work with the District in processing challenges to the accuracy of PII in the custody of the Recipient.

(5) Whether the PII will be stored in the US or outside of the US (and if outside of the US, where), and the security protections taken to ensure such data will be protected (described in such a manner as to protect data security), including whether such data will be encrypted: The Recipient stores its data in the United States and takes strong measures to keep data safe and secure. The Recipient 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 Recipient 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 Recipient 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 Recipient'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 Recipient'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. Recipient limits access to PII 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 Recipient. Anyone involved in the handling of PII 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 Recipient will maintain access log(s) that record all disclosures of or access to PII within its possession and will provide copies of those access log(s) to the District upon request. In addition, the Recipient provides employee training on privacy and data security laws and best practices. If there is any disclosure or access to any PII by an unauthorized party, the Recipient will promptly notify any affected schools and will use reasonable efforts to cooperate with their investigations of the incident.