Clever New York Education Law Section 2-d Addendum

This New York Education Law Section 2-d Addendum (this "*Addendum*") is entered into by and between Henry Johnson Charter School (the "*District*") and Clever Inc. ("*Vendor*") effective as of 10/1/2020. The District on the one hand, and Vendor on the other hand, agree that they shall be bound by the Clever General Terms of Use (including the Privacy Policy and Additional Terms of Use for Schools referenced therein) found at https://clever.com/trust/terms (collectively, the "*Terms*"). This Addendum supplements the Terms, and is hereby incorporated by reference therein, and is being entered into by the parties to ensure that the Terms conform to the requirements of New York Education Law Section 2-d and Section 121.1 of the Regulations of the Commissioner of Education (collectively, "*NY 2-d*"). In the event of a direct conflict between this Addendum and the Terms, this Addendum shall control. For the sake of clarity, except where prohibited by applicable law, any limitations on liability set forth in the Terms shall apply to this Addendum. The Terms and this Addendum shall collectively be referred to herein as the "*Agreement*."

1. Definitions. As used herein, "*Protected Data*" means Student Data (as defined in NY 2-d) and/or Teacher or Principal Data (as defined in NY 2-d). All other capitalized terms used herein shall have the meanings given to them in NY 2-d.

2. Vendor's Obligations and Confidentiality.

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Agreement originates from the District and that as between the parties, such Protected Data belongs to and is under the control of the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including NY 2-d) and the District's policy on data security and privacy (a copy of which has been, or will be, provided to the Vendor by the District).

(c) Vendor will not sell Personally Identifiable Information nor use or Disclose it for any Marketing or Commercial Purpose or facilitate its use or Disclosure by any other party for any Marketing or Commercial Purpose or permit another party to do so.

(d) Vendor will limit internal access to Education Records to those individuals that are determined to have legitimate educational interests within the meaning of NY 2-d and the Family Educational Rights and Privacy Act (FERPA). Vendor will limit internal access to Personally Identifiable Information to only those employees or subcontractors that need access to provide the contracted services.

(e) Vendor will not use Education Records or Personally Identifiable Information for any other purposes than those explicitly authorized in the Agreement.

(f) Except for authorized representatives of Vendor such as a subcontractor or assignee to to the extent they are carrying out the Agreement and in compliance with state and federal law, regulations, and the Agreement, Vendor will not Disclose any Personally Identifiable Information to any other party unless: (i) the disclosure is consistent with the features and functionality of the contracted services being provided to the District or is otherwise directed or authorized by the District; (ii) the Parent or Eligible Student has provided prior written consent; or (ii) the disclosure is required by statute or court order and Vendor provides a notice of the Disclosure to the District no later than the time the Personally Identifiable Information is Disclosed, unless providing notice of the Disclosure is expressly prohibited by the statute or court order.

(g) Vendor shall maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Personally Identifiable Information in its custody. Vendor's safeguards, technologies, and practices will align with the NIST Cybersecurity Framework. Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States.

(h) Vendor will protect Personally Identifiable Information in its custody while in motion or at rest, using an encryption technology or methodology that complies with the requirements of NY 2-d.

(i) Vendor and its assignees who have access to Protected Data have received or will receive training on the federal and state law governing confidentiality of such Protected Data prior to receiving access.

3. Deletion or Disposition of Protected Data Upon Termination. Within sixty (60) days of the expiration of the Terms without renewal, or termination of the Terms prior to their expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor and instruct any of its subcontractors or other authorized persons or entities to whom it has Disclosed Protected Data to securely delete or otherwise destroy any and all Protected Data in their possession. Upon request, Vendor will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

4. Data Security and Privacy Plan. Vendor will maintain a Data Security and Privacy Plan that complies with the requirements set forth in NY 2-d (the "*Vendor Plan*"), which Vendor Plan is attached as Exhibit A hereto.

5. Subcontractors. In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will Disclose the Protected Data to execute legally binding agreements providing for levels of security and confidentiality no less stringent than the data protection, privacy, and security obligations required of Vendor in this Addendum. Vendor shall remain responsible for compliance with its obligations under the Agreement and will be liable to the District for the acts and omissions of any subcontractor or other person or entity to whom Vendor has disclosed or permitted to access Protected Data as if they were the acts and omissions of the Vendor.

6. Notification of Breach and Unauthorized Release.

(a) Vendor shall promptly notify the District of any breach of security resulting in a n Breach or Unauthorized Release of Protected Data by Vendor or its assignees (an "Incident") in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of such Incident. Such required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the Incident; the dates of the Incident and the date of discovery, if known; a description of the types of Protected Data affected; an estimate of the number of records affected; a brief description of Vendor's investigation or plan to investigate; and contact information for representatives who can assist Parents or Eligible Students that have additional questions. Vendor will provide such notification to the District by contacting Emily Wager, Data Protection Officer directly by email at ewager@henryjohnsoncs.org or by calling (518)432-4300 x 211.

(b) Vendor will cooperate with the District and law enforcement to protect the integrity of investigations into the Incident.

(c) Where an Incident is attributable to Vendor, Vendor shall pay or promptly reimburse the District for the full cost of any notifications required to be given by the District under NY 2-d to affected Parents, Eligible Students, teachers, and/or principals.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the Educational Agency with which Vendor contracts, has an obligation under NY 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("*CPO*"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the Incident after having been initially informed of the Incident by the District, Vendor will promptly inform the Data Protection Officer listed in subsection (a) above or his/her designee.

7. Parents Bill of Rights. The parties agree that the District's Parents' Bill of Rights for Data Privacy and Security attached hereto as Exhibit B, and the Parents' Bill of Rights for Data Privacy and Security: Supplemental Information attached hereto as Exhibit C, are incorporated as part of this Addendum.

IN WITNESS OF THE FOREGOING, the duly authorized representatives of the parties have signed this Addendum as of the date set forth above.

Clever Inc.

DocuSigned by:
Kevin Laughlin
37251B4332534F9...

By: ______________________

Name: Kevin Laughlin
Title: CFO

2020-10-20

Henry Johnson Charter School

By: ______________________

Name: Dustin Mitchell
Title: Head of School

EXHIBIT A

Clever Data Security and Privacy Plan

New York Education law §2-d(5)(e)

Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.

1. Clever complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of personally identifiable information and Student Data

The protection of the privacy and confidentiality of Student Data is tremendously important to Clever. Student Data means any information (in any format) that is directly related to any identifiable current or former student that is maintained by Clever for, or on behalf of, its customers.

Clever complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of personally identifiable information and Student Data, including the Federal Family Educational Rights and Privacy Act ("**FERPA**"), 20 U.S.C. § 1232(g); Children's Online Privacy Protection Act ("**COPPA**"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("**PPRA**"), 20 U.S.C. 1232; and applicable State laws governing the protection of personally identifiable information from students' educational records, including New York Educational Law Section 2-d and Part 121 of the Commissioner's Regulations. In particular, Clever:

- Limits internal access to education records to those individuals that are determined to have legitimate educational interests
- Does not use education records for any other purposes than those explicitly authorized in contracts
- Except for authorized representatives and subcontractors, does not disclose any personally identifiable information to any other party without the consent of the parent or eligible student or unless required by statute or court order and the educational agency has been given notice of the disclosure
- Maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in our custody

- Does not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose and will not facilitate the use or disclosure of Personally Identifiable Information (PII) by any other party for marketing or commercial purposes.

When Clever contracts with an educational agency, district or BOCES in the State of New York, Clever agrees to comply with the data security and privacy policy of the agency, district of BOCES and the Parents Bill of Rights for Data Privacy and Security, which is incorporated into the agreement between Clever and the agency, district or BOCES. For the purposes of compliance with the laws and regulations of New York, “Student Data” also means “student data” and “teacher or principal data” as such terms are defined by New York Education Law 2-d.

2. Clever implements administrative, operational and technical safeguards and practices to protect the confidentiality and security of PII and Student Data

Administrative:
Clever limits access to PII only to employees who have a legitimate need to access such data, in order to perform their job functions. For employees, agents and contractors who will access or process Student Data, Clever provides employee training on privacy and data security laws and best practices on a yearly basis and has implemented disciplinary processes for violations of our information security or privacy requirements. Upon termination or applicable role change, we promptly remove data access rights and/or require the return or destruction of data. Additionally, Clever conducts an annual security audit.

Technical:
Clever has adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework. Additionally, Clever uses encryption technology to protect student information while in transit and at rest. While in transit, Clever uses TLS with strong ciphers, with a preference for those with perfect-forward secrecy. While at rest, Clever uses modern cryptographic algorithms (AES256-GCM) and follows key management best practices, with strict user access control to keys. This ensures that the PII requires a particular key to decrypt and encrypt. Additionally, the controls to access and modify these keys are kept secure.

Clever's infrastructure runs on Amazon Web Services (AWS), an industry leader in cloud services and data security. AWS, and other cloud services, have experience in: running and securing servers in the cloud for many customers, navigating and managing security standards, as well as investment in network and physical security. Ernst & Young LLP performs the AWS System and Organization Controls audit, and has a publicly available report on how they meet these compliance controls and objects at https://aws.amazon.com/compliance/soc-faqs/.

Clever employs physical security controls, such as access controls to secure environments and virtual access controls including role-based authentication and strong password policies. Clever also utilizes secure development lifecycle practices, having security protocols inform every aspect of product and infrastructure development. This includes threat modeling and code review for major changes, separation of development and production environments, automated log collection and audit trails for production systems, and policies and procedures for network and operations management. Clever performs annual vulnerability assessments and cloud infrastructure audits..

Clever also maintains a business continuity program, with data backup and recovery capability that is designed to provide a timely restoration of Clever services with minimal data loss in the event of a catastrophic failure or disaster.

3. Compliance with the Supplement to the Parent's Bill of Rights

We comply with the obligations and representations set forth in the Supplement to the Parent's Bill of Rights. See "Supplement."

4. Clever has implemented employee training on privacy and security obligations.

Clever yearly provides employee training on privacy and data security laws and best practices on both the federal and state level. Additionally, we train new employees as a part of onboarding. Access to sensitive data systems is gated upon completion of privacy and security training.

5. Clever oversight of, and responsibility for, sub-contractors

Clever 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 Clever or on Clever's behalf. Clever requires subcontractors to be contractually bound to uphold the same standards for security, privacy, and compliance as are imposed on Clever by applicable state and federal laws and contracts. Clever reviews subcontractor contracts annually. Clever maintains 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. Clever will make available a list of all such subcontractors upon request.

6. Security incident response plan

Clever has an information security incident management protocol to detect, assess, mitigate and respond to security incidents and threats. If Clever believes that there has been unauthorized acquisition or disclosure that compromises the security, integrity or confidentiality of a customer's personal information, we will take all necessary steps to notify the affected customers of the incident as quickly as possible, and in no case greater than two business days after we learn of the breach. Once the communication has been drafted and finalized, within 72 hours of discovery of the incident in the absence of any statutes or custom agreements, we will use Clever's standard outgoing email systems to send the email to the address associated with the Clever district account owner.

To the extent known, this notice will identify (i) the nature of the Security Incident, (ii) the steps we have executed to investigate the Security Incident, (iii) the type of personal information affected, (iv) the cause of the Security Incident, if known, (v) the actions we have taken or will take to remediate any deleterious effects of the Security Incident, and (vi) any corrective actions we have taken or will take to prevent a future Security Incident.

If the incident triggers any third party notice requirements under applicable laws, Clever will comply with its notification obligations under applicable law and the terms of its contractual agreement with the customer.

EXHIBIT B
District's Parents' Bill of Rights

The Henry Johnson Charter School's Parent's Bill of Right can be located on the Henry Johnson Charter School's website at http://www.henryjohnsoncs.org/wp-content/uploads/2020/10/Parents-Bill-of-Rights.pdf

Exhibit C

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

Third Party Contractor: Clever, Inc.(the "*third-party contractor*")
Educational Agency: Henry Johnson Charter School (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. The terms used herein shall have the meanings given to them in New York Education Law §2-d and its implementing regulations. In accordance with these provisions, it is necessary for the third-party contractor 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 the third-party contractor's services to the District. The third-party contractor provides employee training on privacy and data security laws and best practices. To the extent that third-party contractor discloses student data or teacher or principal data to subcontractors, it requires those subcontractors to execute legally binding agreements providing for levels of security and confidentiality that are no less stringent than the data protection, privacy, and security obligations imposed on the third-party contractor by applicable laws (including NY 2-d), and its contract with the District.

(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 contract with the District expires when terminated in accordance with its terms. Within sixty (60) days of the expiration of the contract without renewal, or termination of the contract prior to its expiration, the third-party contractor will securely delete or otherwise destroy any and all student data or teacher or principal data remaining in the possession of the third-party contractor and instruct any of its subcontractors or other authorized persons or entities to whom it has disclosed student data or teacher or principal data to securely delete or otherwise destroy any and all student data or teacher or principal data in their possession.

(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:

A parent or eligible student may challenge the accuracy of the student data or teacher or principal data that is in the custody of the third-party contractor by contacting the student’s District in accordance with the District’s procedures for requesting amendment to educational records under FERPA. Teachers and principals may be able to challenge the accuracy of personally identifiable information provided to the third-party contractor by directing such requests to the District. 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. To protect student data or teacher or principal data stored in its servers, the third-party contractor maintains strict administrative, technical, and physical procedures that align with the NIST Cybersecurity Framework and may include, but are not necessarily limited to, disk encryption, file encryption, firewalls, password protection, and access controls.

(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.