DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including
Washington-Saratoga-Warren-Hamilton-Essex BOCES Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
Washington-Saratoga-Warren-Hamilton-Essex BOCES and Clever, Inc.

1. **Purpose**

(a) **Washington-Saratoga-Warren-Hamilton-Essex BOCES, and on behalf of its subscribed school districts (see Exhibit B)** (hereinafter "District") and **Clever, Inc.** (hereinafter "Vendor") 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 "CLEVER Terms of Service" pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District and/or a Participating School (as defined below) for purposes of providing certain products or services to the District and/or Participating Schools (the "Master Agreement"). For the sake of clarity, unless prohibited by Section 2-d, any limitations on liability set forth in the Master Agreement shall apply to this Data Sharing and Confidentiality Agreement.

(b) This Data Sharing and Confidentiality Agreement supplements the Master Agreement and is considered a part thereof, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This DSA includes a copy of the District's Bill of Rights for Data Security and Privacy attached as Exhibit A hereto signed by Vendor, and the Supplemental Information about the Master Agreement included as Attachment 1 to Exhibit A between **Washington-Saratoga-Warren-Hamilton-Essex BOCES and its subscribed school districts (see Exhibit B)** and **Clever, Inc.** that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this DSA. To the extent that any terms contained in the Master Agreement, or any terms contained in any

other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this DSA, the terms of this DSA will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District and/or a Participating School pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District and/or Participating Schools pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District or a Participating School, as applicable, and that this Protected Data belongs to and is owned by the District or the Participating School, respectively.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy attached hereto as Exhibit C.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District and/or Participating Schools.

Vendor's Plan for protecting the District's and/or Participating Schools' Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's and/or Participating Schools' Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this DSA, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District and/or Participating Schools under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this DSA below entitled "Supplemental Information about a Master Agreement between **Washington-Saratoga-Warren-Hamilton-Essex BOCES** and **Clever, Inc.**" Vendor's obligations described within this section include, but are not limited to:

i. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements that provide for the same level of data protection obligations imposed on Vendor by state and federal law and the Master Agreement, and
ii. its obligation to follow certain procedures for the deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees who will have access to Protected Data, prior to their receiving access, and Vendor's subcontractors or assignees will provide such training to their respective officers and employees who will have access to Protected Data.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District and/or the affected Participating Schools of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement. As used herein, the terms "breach," "unauthorized release" and "unauthorized disclosures" shall have the meanings given to those under in Section 2-d.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District and the affected Participating Schools of any breach or unauthorized release of Protected Data it has received from the District and/or a Participating School in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting **Dr. Turina Parker, Executive Director for Educational and Support Programs** directly by email at **tuparker@wswheboces.org** or by calling **518-581-3717**

(c) Vendor will cooperate with the District and provide as much information as reasonably possible directly to **Dr. Turina Parker** or his/her designee about the incident, including (if and to the extent known) but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 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 **Dr. Turina Parker** or his/her designee.

6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District and/or Participating Schools, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this DSA:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District and/or Participating Schools under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and/or Participating Schools and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District and/or Participating Schools no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part

(h) To not sell Protected Data 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.

(i) To notify the District and/or affected Participating Schools, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policy on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Data Sharing and Confidentiality Agreement.

(j) To cooperate with the District and/or affected Participating Schools and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District and/or affected Participating Schools for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor .

7. **Participating Schools.**

Any of the the subscribed school districts listed in Exhibit B may bind itself and Vendor to the terms of this Data Sharing and Confidentiality Agreement by opting into the terms hereof by informing the District of its desire to do so and by signing the Joinder Agreement attached as Exhibit D hereto

(the "Joinder") and returning a signed copy to the District and Vendor as described in the Joinder. Any subscribed school district that has so signed and returned such a Joinder will be referred to herein as a "Participating School."

8. **Termination.**

For the sake of clarity, (i) any termination of the Master Agreement as it applies between Vendor and a particular Participating School shall not serve to terminate the Master Agreement as it applies between Vendor and the District or Vendor and any other Participating School, and (ii) any termination of the Master Agreement between Vendor and the District as it applies between Vendor and the District shall not terminate this Agreement between Vendor and any Participating School.

In witness of the foregoing, the duly authorized representatives of the parties have signed this Data Sharing and Confidentiality Agreement as of the date set forth above.

Clever Inc.	**Washington-Saratoga-Warren-Hamilton-Essex BOCES**
By: Kevin Laughlin	**By:**
Name: Kevin Laughlin	**Name: Anthony Mueller**
Title: CFO	**Title: Deputy Superintendent**

Washington-Saratoga-Warren-Hamilton-Essex BOCES
Bill of Rights for Data Security and Privacy

The **Washington-Saratoga-Warren-Hamilton-Essex BOCES** 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, the District informs the school community of the following:

Parents and eligible students[1] can expect the following:

1. A student's personally identifiable (PII)[2] information cannot be sold or released for any commercial purposes.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws,[3] such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of personally identifiable information PII, 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 NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed.
   a. Contact WSWHE BOCES Data Protection Officer: **Dr. Turina Parker,** Executive Director of Student Support Services by email: tuparker@wswheboces.org, or by phone: 518-581-3717. Complaints should be submitted in writing using the district form that is available on the BOCES website and in the BOCES offices.
   b. Complaints may also be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

---

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data

---

BY THE VENDOR:

___Kevin Laughlin_____	_____Kevin Laughlin_____
Name (Print)	**Signature**
___CFO, Clever, Inc._____	_____8/7/20_____
Title	**Date**

Attachment 1 to
Exhibit A

Supplemental Information about a Master Agreement between

Washington-Saratoga-Warren-Hamilton-Essex BOCES and Clever, Inc.

Washington-Saratoga-Warren-Hamilton-Essex BOCES and its subscribed school districts (see Exhibit B) has entered into a Master Agreement with **Clever, Inc.**, which governs the availability to the District of the following products or services:

Clever software, applications, technology tools, and/or web-services

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master 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 acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences when agreed to by the parties and continues in effect until terminated as provided for therein.

- Within sixty (60) days of the expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data.

- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, on any storage medium whatsoever after the period ending sixty (60) days from the termination of the Master Agreement. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: 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. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

Exhibit B:

School Districts Subscribed to the Washington-Saratoga-Warren-Hamilton-Essex BOCES Data Privacy & Security and/or Educational Technology and/or School Library Systems Cooperative Service Agreement(s)

Component School Districts

Argyle Central School
Ballston Spa Central School
Bolton Central School
Cambridge Central School
Corinth Central School
Fort Ann Central School
Fort Edward Union Free School
Galway Central School
Glens Falls City School
Glens Falls Common District
Granville Central School
Greenwich Central School
Hadley-Luzerne Central School
Hartford Central School
Hudson Falls Central School
Indian Lake Central School
Johnsburg Central School
Lake George Central School
Mechanicville City School
Minerva Central School
Newcomb Central School
North Warren Central School
Queensbury Union Free School
Salem Central School
Saratoga Springs City Schools
Schuylerville Central School
South Glens Falls Central School
Stillwater Central School
Warrensburg Central School
Waterford-Halfmoon Union Free School
Whitehall Central School

Other Subscribing School Districts

Beekmantown Central School District
Bethlehem Central School District
Broadalbin Central School District
Deposit Central School District
Fort Plain Central School District
Greater Amsterdam School District
Johnstown Central School District
NorthEast Clinton Central School District
Ravena Coeymans Selkirk School District
Rensselaer City School District
Shenendehowa Central School District
Voorheesville Central School District

EXHIBIT C: Washington-Saratoga-Warren-Hamilton-Essex BOCES
Board of Education Policy #6810: Privacy & Security of Student Data, Teacher & Principal Data

(see attached)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The Board of Cooperative Educational Services ("BOCES") is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the BOCES and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The BOCES adopts this policy to implement the requirements of Education Law Section 2-d and Part 121 of the Commissioner's Regulations (hereinafter "implementing regulations"), as well as to align the BOCES' data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c d.

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c d.

d) "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f) "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g) "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) "Eligible student" means a student who is eighteen years or older.

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m) "Parent" means a parent, legal guardian, or person in parental relation to a student.

n) "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

o) "Release" shall have the same meaning as disclosure or disclose under this policy.

p) "Student" means any person attending or seeking to enroll in an educational agency.

q) "Student data" means personally identifiable information from the student records of an educational agency.

r) "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.

s) "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district or BOCES to carry out its responsibilities pursuant to Education Law

Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

t) "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the BOCES will take steps to minimize its collection, processing, and transmission of PII. Additionally, the BOCES will:

a) Not sell PII 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.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and BOCES policy.

c) Ensure that every use and disclosure of personally identifiable information by the BOCES shall benefit its students and the BOCES (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

d) Ensure that personally identifiable information is not included in public reports or other documents.

Except as required by law or in the case of educational enrollment data, the BOCES will not report to NYSED the following student data elements:

a) Juvenile delinquency records;

b) Criminal records;

c) Medical and health records; and

d) Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the BOCES.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and

principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The BOCES will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer's powers and duties shall not exceed those provided in Education Law Section 2-d and its implementing regulations.

Data Protection Officer

The BOCES has designated the Executive Director for Educational and Support Programs to serve as the BOCES Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions.

Data Privacy and Security Standards

The BOCES will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

The BOCES will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by the BOCES benefits students and the BOCES by considering, among other criteria, whether the use and/or disclosure will:

   1. Improve academic achievement;

   2. Empower parents and students with information; and/or

   3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

The BOCES affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-Party Contractors

BOCES Responsibilities

The BOCES will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the BOCES, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and BOCES policy.

In addition, the BOCES will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the BOCES.

The third-party contractor's data privacy and security plan must, at a minimum:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with BOCES policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;

e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the BOCES;

g) Describe whether, how, and when data will be returned to the BOCES, transitioned to a successor contractor, at the BOCES' option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the BOCES under which the third-party contractor will receive student data or teacher or principal data from the BOCES, is required to:

a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b) Comply with BOCES policy and Education Law Section 2-d and its implementing regulations;

c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the BOCES; or

2. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g) Use encryption to protect PII in its custody while in motion or at rest; and

h) Not sell PII 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.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Click-Wrap Agreements

Periodically, BOCES staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

BOCES staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the BOCES unless they have received prior approval from the BOCES' Data Privacy Officer or designee.

The BOCES will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

Pursuant to Part 121 of the Commissioner's Regulations, the BOCES shall create and publish a Parent's Bill of Rights for Data Privacy and Security ("Bill of Rights") to its website. The BOCES will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the BOCES. For each contract the BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the BOCES, the BOCES will include the necessary supplemental information as required by Part 121 of the Commissioner's Regulations.

The BOCES will publish the supplemental information to the Bill of Rights on its website, for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the BOCES. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the BOCES' data and/or technology infrastructure.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the BOCES under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the BOCES in a manner prescribed by the BOCES.

The BOCES will ensure that only authorized individuals are able to inspect and review student data. To that end, the BOCES will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the BOCES and not to a third-party contractor. The BOCES may require that requests to inspect and review education records be made in writing.

The BOCES will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the BOCES through its annual FERPA notice. A notice separate from the annual FERPA notice is not required.

The BOCES will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The BOCES may provide the records to a parent or eligible student electronically, if the parent consents. The BOCES must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The BOCES will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to

the Chief Privacy Officer at NYSED. In addition, the BOCES administration is responsible for developing procedures for parents, eligible students, teachers, principals, and other BOCES staff to file complaints with the BOCES about breaches or unauthorized releases of student data and/or teacher or principal data.

These procedures are provided in the Administrative Regulation to this policy, and will also be disseminated to parents, eligible students, teachers, principals, and other BOCES staff.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Reporting a Breach or Unauthorized Release

The BOCES will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the BOCES to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the BOCES will be required to promptly notify the BOCES of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, BOCES policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the BOCES will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Notification of a Breach or Unauthorized Release

The BOCES will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the BOCES or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the BOCES will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

b) A description of the types of PII affected;

c) An estimate of the number of records affected;

d) A brief description of the BOCES' investigation or plan to investigate; and

e) Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the BOCES for the full cost of this notification.

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The BOCES may deliver this training using online training tools.

Notification of Policy

The BOCES will publish this policy on its website and provide notice of the policy to all staff.

Education Law § 2-d
8 NYCRR Part 121

Adopted: June 10, 2020

EXHIBIT D

JOINDER AGREEMENT

This Joinder Agreement ("**Joinder**") is effective as of the date of signature below and is entered into by the undersigned Participating School pursuant to that certain Data Sharing and Confidentiality Agreement, dated _____ __, 2020, by and between Clever Inc. and Washington-Saratoga-Warren-Hamilton-Essex BOCES (the "DSA"). Capitalized terms used but not defined in this Joinder shall have the respective meanings ascribed to such terms in the DSA. By the execution of this Joinder, the Participating School (i) agrees to be bound by, and subject to, the terms and conditions of the DSA, (ii) adopts the DSA with the same force and effect as if the Participating School was originally a party thereto, and (iii) agrees that any Protected Data provided by the Participating School to Vendor shall be governed by the DSA.

The DSA shall extend only to the data privacy and security matters that are the subject matter thereof and the Master Agreement shall continue to govern with respect to all other matters. In the event of a conflict or an inconsistency between the terms and conditions of any Master Agreement and the terms and conditions of this DSA, this DSA shall govern and control.

In order for this Joinder to be effective, the Participating School must send a signed copy of this Joinder to Washington-Saratoga-Warren-Hamilton-Essex BOCES via email to cdansereau-rumley@wswheboces.org or by mail to Cecilia Dansereau Rumley, Lead Coordinator for Data Privacy, WSWHE BOCES Student Support Services, 267 Ballard Rd, Suite 5, Wilton NY 12831 and to Vendor via email at trust@clever.com or by mail to Attn: Drew Patterson, Clever, Inc., 1263 Mission Street, San Francisco, California 94103.

Name of Participating School:

By: _____
Name: _____
Title: _____
Date: _____
Address: _____
_____

Clever

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.

7. Clever's responsibility to return or destroy personal information upon termination of the agreement

The agreement with the District expires when terminated in accordance with its terms. Upon the termination of Clever's agreement with the District for any reason, Clever will, as directed by the District in writing, return or 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) all customer PII received by Clever pursuant to the agreement. Unless and to the extent the customer submits a written request to trust@clever.com for the return of PII prior to the termination of the agreement, Clever will automatically delete or de-identify all Student Data within seventy-two (72) hours upon termination of the agreement, except for Student Data residing on backups or internal logs which will be removed within sixty (60) days. In the event the agreement is assigned to a successor contractor in accordance with the terms of the customer agreement, Clever will cooperate with the customer as necessary to transition the PII to the successor contractor prior to deletion.