

## DATA PRIVACY AGREEMENT

**Tupper Lake Central School District**

**and**

**Clever**

This Data Privacy Agreement ("DPA") is by and between the Tupper Lake Central School District ("EA"), an Educational Agency, and Clever, Inc. ("Contractor"), collectively, the "Parties".

### ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** 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.
- 2. 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.
- 3. Disclose:** 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.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or 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 guidance issued under Section 13402(H)(2) of Public Law 111-5.
- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher or principal

APPR data, means personally identifiable information as such term is defined in Education Law §3012-c (10).

- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information from student records of an educational agency.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** 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 § 3012-c and 3012-d.

## ARTICLE II: PRIVACY AND SECURITY OF PII

### 1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated [ June 8, 2022] ("Service Agreement") and Clever's General Terms of Use, Privacy Policy, and Additional Terms of Use for Schools referenced therein, found at <https://clever.com/trust/terms>, (collectively, "Contractor Service Agreements"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

### 2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

### **3. Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

### **4. Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the security practices as described at <https://clever.com/trust/security/practices>.

### **5. Right of Review and Audit.**

Contractor provides the EA with copies of its policies and related procedures that pertain to the protection of PII at <https://clever.com/trust/security/practices>. It is made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

### **6. Contractor's Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point Contractor becomes aware that a subcontractor fails to materially comply with the

requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors, if the subcontractor act or omission is due to Contractor negligence.
- (e) Contractor must not disclose PII to any other party unless:
  - (i) The Contractor has received written permission from a parent or eligible student to whom the data pertains to beforehand; or
  - (ii) Such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

#### **7. Training.**

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

#### **8. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

#### **9. Data Return and Destruction of Data.**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever 60 days after the termination of Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

**10. Commercial or Marketing Use Prohibition.**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

**11. Encryption.**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

**12. Breach.**

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy

to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

- (b) Notifications required under this paragraph must be provided to the EA at the following address:

**Name:** Russell Bartlett

**Title:** Data Protection Officer

**Address:** 294 Hosley Avenue

**City, State, Zip:** Tupper Lake, NY 12986

**Email:** [dpo@tupperlakecsd.net](mailto:dpo@tupperlakecsd.net)

### **13. Cooperation with Investigations.**

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

### **14. Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

### **15. Termination.**

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

## **ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**

### **1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review

any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

**2. Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

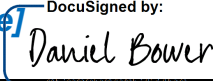
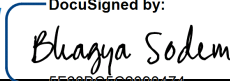
**ARTICLE IV: MISCELLANEOUS**

**1. Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement and Contractor Services Agreements, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

**2. Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
BY: <i>[Signature]</i> DocuSigned by:  <small>3EC92B3C8F474D0...</small>	BY: <i>[Signature]</i> DocuSigned by:  <small>5F885C5C2090474...</small>
<i>[Printed Name]</i> Daniel Bower	<i>[Printed Name]</i> Bhagya Sodem
<i>[Title]</i> Assistant Superintendent for Finance	<i>[Title]</i> Director, District Success, Clever
Date: 2022-10-07	Date: 2022-06-27

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

Education Law §2-d Bill of Rights for Data Privacy and Security for Tupper Lake Central School District Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501- 6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at <http://www.nysed.gov/data-privacy-security/student-data-inventory> and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at <http://www.nysed.gov/dataprivacysecurity/report-improper-disclosure>, by mail to: Data Protection Officer, [dpo@tupperlakecsd.net](mailto:dpo@tupperlakecsd.net), (518) 359-3371 Russell Bartlett Elizabeth Littlefield Cynthia Lauzon Daniel Bower Superintendent Principal/ Director of Special Programs Principal Business Administrator District Office LP Quinn Elementary School Middle/High School District Office.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

<b>CONTRACTOR</b>	
<b>[Signature]</b>	DocuSigned by: <i>Bhagya Sodem</i> 5F68B66C2000474...



<b>[Printed Name]</b>	Bhagya Sodem
<b>[Title]</b>	Director, District Success, Clever
<b>Date:</b>	2022-06-27

## EXHIBIT B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -  
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	Clever, Inc.
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Clever, Inc. provides an application management system offered at no costs to districts subject to the terms and conditions set forth in Clever's Terms of Use (including the Additional Terms of Use for Schools and the Clever Privacy Policy) available at: <a href="https://clever.com/trust/terms">https://clever.com/trust/terms</a> visited on May 10, 2022. The Clever technology system is integrated into the district- student information system and identity system to create easy and secure data transportation for rostering and provisioning of student accounts for partner applications. Clever offers single-sign-on into any application, a customizable student and teacher portal, and an administrator dashboard that allows for easy trouble-shooting and application management.
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input type="checkbox"/> Student PII
<b>Contract Term</b>	Contract Start Date ____ June 8, 2022 ____ Contract End Date ____ June 8, 2025 ____

<b>Subcontractor Written Agreement Requirement</b>	<p>Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)</p> <p><input type="checkbox"/> ›</p> <p><input type="checkbox"/> <b>Contractor will utilize subcontractors.</b></p>
<b>Data Transition and Secure Destruction</b>	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <ul style="list-style-type: none"> <li>• <del>Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</del></li> <li>• <b>Securely delete and destroy data.</b></li> </ul>
<b>Challenges to Data Accuracy</b>	<p>Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.</p>
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> <b>Using a cloud or infrastructure owned and hosted by a third party.</b></p> <p><input type="checkbox"/> ›</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
<b>Encryption</b>	<p>Data will be encrypted while in motion and at rest.</p>

**CONTRACTOR**

<b>[Signature]</b>	DocuSigned by: <i>Bhagya Sodem</i> 5F68BC5C2090474...
<b>[Printed Name]</b>	Bhagya Sodem
<b>[Title]</b>	Director, District Success, Clever
<b>Date:</b>	2022-06-27

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

#### **1. Clever complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of 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 Districts (as defined below).

Clever complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of 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 Student Data 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 Student Data in our custody.
- Does not sell Student Data or use or disclose it for any marketing or commercial purpose and will not facilitate the use or disclosure of Student Data by any other party for marketing or commercial purposes.

When Clever contracts with a district, BOCES, or other educational agency (a "District"), in the State of New York, Clever agrees to comply with the data security and privacy policy of the District and the Parents Bill of Rights for Data Privacy and Security, which is incorporated into the agreement between Clever and the District. 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 Student Data**

**Administrative:**

Clever limits access to Student Data 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 Data 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 Student Data 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, and investing 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 Student Data only to those employees or trusted service providers who have a legitimate need to access such Student 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 makes available a list of all such subcontractors at <https://clever.com/trust/subprocessors>.**

#### **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 District's Student Data, we will take all necessary steps to notify the affected District 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 Student Data 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 District.**

#### **7. Clever's responsibility to destroy Student Data 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 Student Data received by Clever pursuant to the agreement. Unless and to the extent the District submits a written request to [trust@clever.com](mailto:trust@clever.com) for the return of Student Data 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.**