

# **CLEVER STUDENT DATA PRIVACY AGREEMENT**

**Local Education Agency**

**and**

**Clever Inc.**

This Clever Student Data Privacy Agreement (“**DPA**”) is entered into between the Local Education Agency (the “**LEA**”) and Clever Inc. (the “**Provider**”) (each, a “**Party**” and collectively, the “**Parties**”). In consideration of the mutual obligations set out herein, upon signature, the Parties hereby agree that the terms and conditions set out below shall be added as a DPA to the Service Agreement.

#### HOW TO EXECUTE THIS DPA

This DPA has been pre-signed by the Provider. When the Provider receives the completed and signed DPA without modifications as specified below, this DPA will become a legally binding DPA to the Service Agreement. To make this DPA a part of the Service Agreement, LEA must:

1. Complete the information in the signature block of this DPA and have an authorized representative sign; and
2. Submit the completed and signed DPA via email to legal@clever.com.

Any modification will render the signature herein void. If the LEA wants to modify any portion of this DPA, please email legal@clever.com.

**WHEREAS**, the Provider is providing educational or digital services to LEA;

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), and applicable state privacy laws and regulations; and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Exhibits hereto.
2. In the event there is conflict between the terms of this DPA and any other writing, including, but not limited to the Service Agreement, the terms of this DPA shall control.
3. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
4. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail.

## ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.
2. **Parent Access.** To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Educational Records and/or Student Data, correct erroneous information, and transfer student-generated content to a personal account. To the extent LEA cannot access or correct Student Data, Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct, as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, which will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider as part of the Services, Provider shall, at the request of the LEA,

transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (each a “Requesting Party”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Requesting Party to request the Student Data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Requesting Party unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

### **ARTICLE III: DUTIES OF LEA**

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized use or access of the Services or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
5. **LEA Representative.** Any notices, communications, or consents required by or relating to this DPA from Clever to the LEA will be sent to the person(s) listed below (the “Principal Contact Person”). The Principal Contact Person shall be authorized to act on behalf of the LEA and to make decisions for the LEA and shall serve as the representative of the LEA for coordination and fulfillment of the duties of this DPA.

LEA Principal Contact Person:

Name:

Address:

Phone:

Fax:

Email:

#### **ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** The Provider shall comply with all applicable federal and state laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA, to improve the Services, as required by applicable law or court order, and as a result of a merger or acquisition of some or all of its assets or in the diligence process in contemplation thereof.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information or to Student Data disclosed: (1) pursuant to a lawfully issued subpoena or other legal process or (2) to subprocessors performing services on behalf of the Provider in connection with operating, protecting, or improving the Services. Provider will not "Sell" Student Data or "Share" Student Data for purposes of "cross-context behavioral advertising" (as such terms are defined in applicable state privacy laws).
5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De- Identified Data may be used by the Provider for any lawful purpose, including, but not limited to, those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request, unless Provider is required to retain such information to resolve disputes, enforce its agreements, or comply with its legal obligations or with law enforcement requests. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data within a reasonable amount of time. The duty to dispose of Student Data shall not extend to Student Data that has been De-Identified or placed in a separate student account pursuant to Section II 3.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to
  - (a) inform, influence, or enable Targeted Advertising; or
  - (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Services to LEA or as set forth in the Service Agreement. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Student Data shall be stored within the United States.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data. The Provider will cooperate reasonably with  
  
the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the delivery of Services to the LEA.
3. **Data Security.**
  - (1) **By Provider.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on NIST Cybersecurity Framework (CSF) v1.1

- (2) **By LEA.** LEA and its users are solely responsible for choosing secure credentials ("Access Credentials") to access the Services and for keeping such Access Credentials confidential. LEA is responsible for any use of the Services using its and its users' Access Credentials, except to the extent such Access Credentials were obtained directly from Provider.

4. **Security Incident.** In the event that Provider becomes aware of any actual or reasonably suspected unauthorized access to, or unauthorized release, disclosure or acquisition of, Student Data (other than unauthorized access to, or unauthorized release, disclosure, or acquisition of, Student Data resulting from the LEA's failure to keep its Access Credentials secure or confidential as set forth in section 3(2) above) that compromises the security, confidentiality or integrity of the Student Data ("**Security Incident**") maintained by the Provider, the Provider shall provide notification to the impacted LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The Security Incident notification described above shall include the following information to the extent known by the Provider and as it becomes available:
  - i. A list of the types of personal information that were or are reasonably believed to have been the subject of a Security Incident.
  - ii. Either (1) the date of the Security Incident , (2) the estimated date of the Security Incident , or (3) the date range within which the Security Incident occurred.
  - iii. Whether the notification was delayed as a result of a law enforcement investigation or request, if permitted.
  - iv. A general description of the Security Incident,
- (2) Provider agrees to adhere to all federal and state legal requirements with respect to a Security Incident, including, when required, the responsibilities and procedures for notification and mitigation of any such Security Incident.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Security Incident and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) In the event of a Security Incident originating from LEA's use of the Services, Provider shall make information available to LEA to the extent reasonably necessary to allow the LEA to secure Student Data.

## ARTICLE VI: MISCELLANEOUS

1. **Termination.** In the event that either party seeks to terminate this DPA, they may do so so long as the LEA terminated its use of Provider's Service. The Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
2. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA.
3. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
4. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
5. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
6. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition,

consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

7. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
8. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

IN WITNESS WHEREOF, the parties have executed this Student Data Privacy Agreement as of the last day noted below.

**Provider:** Clever Inc.

**LEA:** \_\_\_\_\_

DocuSigned by:  
  
6F09436D82772603...  
\_\_\_\_\_  
(Authorized Signature)  
Wendy Yu  
\_\_\_\_\_  
(Name)  
Head of Legal and Privacy  
\_\_\_\_\_  
(Title)  
trust@clever.com  
\_\_\_\_\_  
(Email)  
585 Market St, Suite 1850,  
San Francisco, CA 94105  
\_\_\_\_\_  
(Address)  
2023-03-03  
\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Authorized Signature)  
\_\_\_\_\_  
(Name)  
\_\_\_\_\_  
(Title)  
\_\_\_\_\_  
(Email)  
\_\_\_\_\_  
(Address)  
\_\_\_\_\_  
(Date)

## **EXHIBIT “A”**

### **DESCRIPTION OF SERVICES**

Provider provides an application management system offered at no cost to districts subject to the Service Agreement available at: <https://clever.com/about/terms>. Provider's 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. Provider 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.

## EXHIBIT “B”

### SCHEDULE OF DATA

| Category of Data                    | Elements   | Check if Used by Your System        |
|-------------------------------------|--|-------------------------------------|
| Application Technology Meta Data    | IP Addresses of users, Use of cookies, etc.  | <input checked="" type="checkbox"/> |
|                                     | Other application technology meta data-Please specify:   | <input type="checkbox"/>            |
| Application Use Statistics          | Meta data on user interaction with application: If the LEA opts in, Provider can report aggregate analytics about student usage of other apps. | <input checked="" type="checkbox"/> |
| Assessment                          | Standardized test scores   | <input type="checkbox"/>            |
|                                     | Observation data   | <input type="checkbox"/>            |
|                                     | Other assessment data-Please specify:  | <input type="checkbox"/>            |
| Attendance                          | Student school (daily) attendance data; LEA must opt-in  | <input checked="" type="checkbox"/> |
|                                     | Student class attendance data; LEA must opt-in   | <input checked="" type="checkbox"/> |
| Communications                      | Online communications captured (emails, blog entries)  | <input checked="" type="checkbox"/> |
| Conduct                             | Conduct or behavioral data   | <input type="checkbox"/>            |
| Demographics                        | Date of Birth, optional  | <input checked="" type="checkbox"/> |
|                                     | Place of Birth   | <input type="checkbox"/>            |
|                                     | Gender, optional   | <input checked="" type="checkbox"/> |
|                                     | Ethnicity or race, optional  | <input checked="" type="checkbox"/> |
|                                     | Language information (native, or primary language spoken by student), optional   | <input checked="" type="checkbox"/> |
|                                     | Other demographic information-Please specify:  | <input type="checkbox"/>            |
| Enrollment                          | Student school enrollment  | <input checked="" type="checkbox"/> |
|                                     | Student grade level, optional  | <input checked="" type="checkbox"/> |
|                                     | Homeroom, optional   | <input checked="" type="checkbox"/> |
|                                     | Guidance counselor   | <input type="checkbox"/>            |
|                                     | Specific curriculum programs   | <input type="checkbox"/>            |
|                                     | Year of graduation, optional   | <input checked="" type="checkbox"/> |
|                                     | Other enrollment information-Please specify:   | <input type="checkbox"/>            |
| Parent/Guardian Contact Information | Address  | <input type="checkbox"/>            |
|                                     | Email, optional  | <input checked="" type="checkbox"/> |
|                                     | Phone, optional  | <input checked="" type="checkbox"/> |
| Parent/Guardian ID                  | Parent ID number (created to link parents to students)   | <input checked="" type="checkbox"/> |

|                      |                             |                                     |
|----------------------|-----------------------------|-------------------------------------|
| Parent/Guardian Name | First and/or Last, optional | <input checked="" type="checkbox"/> |
| Schedule             | Student scheduled courses   | <input checked="" type="checkbox"/> |

|                             |  |                                     |
|-----------------------------|--|-------------------------------------|
|                             | Teacher names  | <input checked="" type="checkbox"/> |
| Special Indicator           | English language learner information, optional   | <input checked="" type="checkbox"/> |
|                             | Low-income status  | <input type="checkbox"/>            |
|                             | Medical alerts/ health data  | <input type="checkbox"/>            |
|                             | Student disability information   | <input type="checkbox"/>            |
|                             | Specialized education services (IEP or 504), optional  | <input checked="" type="checkbox"/> |
|                             | Living situations (homeless/foster care)   | <input type="checkbox"/>            |
|                             | Other indicator information-Please specify:  | <input type="checkbox"/>            |
| Student Contact Information | Address, optional  | <input checked="" type="checkbox"/> |
|                             | Email, optional  | <input checked="" type="checkbox"/> |
|                             | Phone  | <input type="checkbox"/>            |
| Student Identifiers         | Local (School district) ID number  | <input checked="" type="checkbox"/> |
|                             | State ID number, optional  | <input checked="" type="checkbox"/> |
|                             | Provider/App assigned student ID number  | <input checked="" type="checkbox"/> |
|                             | Student app username   | <input checked="" type="checkbox"/> |
|                             | Student app passwords  | <input checked="" type="checkbox"/> |
| Student Name                | First and/or Last  | <input checked="" type="checkbox"/> |
| Student In App Performance  | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | <input type="checkbox"/>            |
| Student Program Membership  | Academic or extracurricular activities a student may belong to or participate in                                       | <input type="checkbox"/>            |
| Student Survey Responses    | Student responses to surveys or questionnaires   | <input type="checkbox"/>            |
| Student work                | Student generated content; writing, pictures, etc.   | <input type="checkbox"/>            |
|                             | Other student work data -Please specify:   | <input type="checkbox"/>            |
| Transcript                  | Student course grades  | <input type="checkbox"/>            |
|                             | Student course data  | <input type="checkbox"/>            |
|                             | Student course grades/ performance scores  | <input type="checkbox"/>            |
|                             | Other transcript data - Please specify:  | <input type="checkbox"/>            |
| Transportation              | Student bus assignment   | <input type="checkbox"/>            |
|                             | Students pick up and/or drop off location  | <input type="checkbox"/>            |

|       |  |                          |
|-------|--|--------------------------|
|       | Student bus card ID number   | <input type="checkbox"/> |
|       | Other transportation data – Please specify:  | <input type="checkbox"/> |
| Other | Please list each additional data element used, stored, or collected by your application: Messages sent via Provider Messaging if LEA does not opt-out. | <input type="checkbox"/> |
| None  | No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.                              | <input type="checkbox"/> |

## **EXHIBIT “C”**

### **DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, test protocols and individualized education programs.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Student Generated Content:** The term “student-generated content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re- disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the General Terms of Use, Additional Terms of Use for Schools, and Privacy Policy.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that can reasonably be used to identify or contact a particular student, including, but not limited to, information in the Educational Record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents’ names, or any other information or identification number that would provide information about a specific student. Student Data further includes “personally identifiable information (PII),” as defined in 34

C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit “B”** is confirmed to be collected or processed by the Provider pursuant to the Services and as described in this DPA. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

**Subprocessor:** For the purposes of this DPA, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term “Third Party” means a provider of digital educational software or services, including cloud- based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term “Third Party” when used to indicate the provider of digital educational software or services is replaced by the term “Provider.”

## **EXHIBIT “D”**

### **DATA SECURITY REQUIREMENTS**

Clever complies with its responsibilities under all applicable state and federal laws and regulations that protect the confidentiality of Student Data. Clever outlines its securities policies at: <https://clever.com/trust/security> and <https://clever.com/trust/security/practices>.

Adequate Cybersecurity Frameworks 2/24/2020

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* (“Cybersecurity Frameworks”) that may be utilized by Provider.

Cybersecurity Frameworks

| <input type="checkbox"/>            | <b>MAINTAINING ORGANIZATION/GROUP</b>  | <b>FRAMEWORK(S)</b>  |
|-------------------------------------|--|--|
| <input checked="" type="checkbox"/> | National Institute of Standards and Technology                                       | NIST Cybersecurity Framework Version 1.1   |
| <input type="checkbox"/>            | National Institute of Standards and Technology                                       | NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171 |
| <input type="checkbox"/>            | International Standards Organization   | Information technology — Security techniques — Information security management systems (ISO 27000 series)                      |
| <input type="checkbox"/>            | Secure Controls Framework Council, LLC   | Security Controls Framework (SCF)  |
| <input type="checkbox"/>            | Center for Internet Security   | CIS Critical Security Controls (CSC, CIS Top 20)   |
| <input type="checkbox"/>            | Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) | Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)   |

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

