

CALIFORNIA STUDENT DATA PRIVACY
AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:

Twin Rivers Unified School District

AND

Provider:

Clever, Inc.

Date:

5/28/19

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Twin Rivers Unified School District

(hereinafter referred to as "LEA") and Clever, Inc.
(hereinafter referred to as "Provider") on 5/28/19
the terms as stated herein.

. The Parties agree to

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

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 transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, 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, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:
3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".
4. **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 term used in 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 Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. 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. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (4 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 data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to

attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
- f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance

monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i.** The name and contact information of the reporting LEA subject to this section.
 - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA’s discretion, the security breach notification may also include any of the following:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.
 - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d.** Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

- e. 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 data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is

provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Russ Selken
Title: Executive Director of Inform

Contact Information:
russ.selken@twinriversusd.org
(916) 566-3400

The designated representative for the Provider for this Agreement is:

Name: Carolyn Ajnassian
Title: Director of Customer Succes

Contact Information:
carolyn.ajnassian@clever.com

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: _____
Title: _____

Contact Information:

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes 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.

7. **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.
8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **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.

[Signature Page Follows]

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

Provider: Clever, Inc.

BY: Carolyn Ajrassan Date: 5/28/19

Printed Name: Carolyn Ajrassan Title/Position: Director of Customer Success

Local Education Agency: Twin Rivers Unified School District

BY: Russ Selken Date: 5/31/2019

Printed Name: Russ Selken Title/Position: Executive Director of Infor

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

Provider provides an application management system offered at no cost to School Districts and the LEA subject to the terms and conditions set forth in Provider's Terms of Use (including the Additional Terms of Use for Schools and Privacy Policy) available at: <https://clever.com/about/terms> (the "Service Agreement"), which Service Agreement is hereby incorporated into this DPA. 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. In the event of an express conflict between the Service Agreement and this DPA, this DPA will supersede. The parties agree that the limitation of liability provision set forth in the Service Agreement will apply to and govern this DPA (including Provider's indemnity obligations set forth in this DPA).

Notwithstanding anything to the contrary set forth in this DPA, the parties hereby acknowledge and agree that Developers (as defined in the Service Agreement) shall not be deemed to be "Subprocessors" for purposes of this DPA and that only those third parties who have access to Student Data and Education Records in order to provide some component of the Services (as defined in the Service Agreement) shall be deemed to be Subprocessors under this DPA.

Notwithstanding anything to the contrary set forth in this DPA, the parties hereby acknowledge and agree that Provider owns all metadata and metadata shall under no circumstances be deemed to be "Student Data" or "Personally Identifiable Information" for purposes of this DPA.

Notwithstanding anything to the contrary in this DPA, Provider may disclose Student Data and Education Records in accordance with the Service Agreement.

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.	X
	Other application technology meta data-Please specify:	See Other section below
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
Enrollment	Other demographic information-Please specify:	Hispanic_Latio n
	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X

Parent/ Guardian ID	Parent ID number (created to link parents to students)	X
Parent/ Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	X
	Living situations (homeless/ foster care)	
	Other indicator information- Please specify:	FRL Status
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID	X

	number	
	State ID number	X
	Provider/App assigned student ID number	
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/appli- cation performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student	

	work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/perfor- mance scores	
	Other transcript data -Please specify:	Unweighted GPA, weighted GPA
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	Principal name, principal email, staff ID

No Student Data Collected at this time _____.
 *Provider shall immediately notify LEA if this
 designation is no longer applicable.

OTHER: Use this box, if more space needed.

Other continued: admin email, admin first name, admin last name, admin title, admin user name, admin password, admin role, school city, school address, school state, school zip, school phone, teacher id, state teacher ID, teacher number, teacher first name, teacher last name, teacher username, teacher password, course name, course description, period, subject, term name, term start, term end

For the application technology meta data section - please see the information collected through technology section of Clever's Commitment to Your Privacy at https://clever.com/about/privacy-policy#how_we_collect_and_use_information

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "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 primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. 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.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Twin Rivers Unified School District directs Clever, Inc. to
dispose of data obtained by Provider pursuant to the terms of the Service Agreement
between LEA and Provider. The terms of the Disposition are set forth below:

<u>Extent of Disposition</u> Disposition shall be:	 ☐ Partial. The categories of data to be disposed of are as follows: ☐ Complete. Disposition extends to all categories of data.
<u>Nature of Disposition</u> Disposition shall be by:	 ☐ Destruction or deletion of data. ☒ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
<u>Timing of Disposition</u> Data shall be disposed of by the following date:	 ☒ As soon as commercially practicable ☐ By (Insert Date) _____

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Twin Rivers Unified School and which is dated 5/28/19 to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: Clever, Inc.

BY: Carolyn Ajnassian

Date: 5/28/19

Printed Name: Carolyn Ajnassian

Title/Position: Director of Customer Success

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA: Irvine Unified School District

BY: [Signature]

Date: January 29, 2020

Printed Name: John Fogarty

Title/Position: Asst Supt Business Services

IUSD Board Approved: 11/14/2017

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Carolyn Ajnassian

Title: Director of Customer Success

Email Address: Carolyn.Ajnassian@Clever.com

EXHIBIT "F" DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

Clever General Terms of Use

Effective Date: July 7, 2017

Welcome to Clever! We're delighted to have you on our website and maybe even using our service (the "Services"). Please continue reading to learn about the terms by which you may use our web and/or mobile services (collectively, the "Services"). If you have questions about this Agreement, please contact us by visiting our [Help Center](#).

These General Terms of Use apply to all: (i) schools, school districts, and related entities and organizations that sign up to use the Services, including but not limited to administrators who access the Services on their behalf (each a "School"); (ii) non-School visitors, users, and others, including students, teachers, and their parents, who use the Services; and (iii) third-party providers of applications (each a "Developer" and collectively with the individuals referenced in (ii) above and Schools, the "Users" or "you"). If you're a School, our [Additional Terms of Use for Schools](#) apply to you too. If you're a Developer, our [Additional Terms of Use for Developers](#) apply to you too. These General Terms of Use, the [Additional Terms of Use for Schools](#) (as applicable to Schools) and the [Additional Terms of Use for Developers](#) (as applicable to Developers) are collectively referred to herein as the "Agreement".

By accessing or using the Services, checking the box marked ["I Agree"], or by otherwise affirmatively stating your desire to use the Services, you signify that you have read, understood, and agree to be bound by this Agreement and to the collection and use of your information as set forth in the [Clever Privacy Policy](#), otherwise you may not use the Services. Because our Services change relatively often, the terms in this Agreement and our Privacy Policy may change too. If you are a School or a Developer using the Services, we will notify you via email in advance of any material changes to the terms. Upon making changes, we will update the "Effective Date" found at the top of this page. Your continued use of the Services after any changes constitutes your acceptance of the new terms.

SECTION 1. WHAT ARE CLEVER'S SERVICES AND WHO CAN USE THEM?

What do we do? We provide Schools both data integration and single sign-on functionality, making it easier for Schools to choose, deploy, and control software applications made available by Developers that are used by their teachers and students as well as to use certain software we may make available to access the Services via a mobile device (an "App").

laws, rules and regulations. If you've been removed from the Services previously, you're not allowed to use them again.

Subject to the terms and conditions of this Agreement, Clever grants to you permission to access and use the Services. We reserve all rights not expressly granted to you in the Services and the Clever Content (as defined below). We may terminate this license at any time for any or no reason.

i) DETAILS ABOUT THE CLEVER SERVICES

Your Clever account gives you access to our Services, but don't sign up on behalf of a School if you do not have the requisite authority to do so. Once you sign up, you are responsible for your account and any data associated with it.

Your Clever account gives you access to the Services and functionality we make available from time to time and at our discretion, which may include single sign-on capability for certain applications made available by Developers. We maintain different types of accounts for different types of Users. If you open a Clever account on behalf of a School or a Developer, then (a) "you" includes you and that entity, and (b) you represent and warrant that you are an authorized representative of the entity with the authority to bind the entity to this Agreement and that you agree to this Agreement on the entity's behalf.

Remember: you are responsible for any activity that occurs on your account, you may never use someone else's account without permission, and you must keep your account password secure. We recommend using "strong" passwords (passwords that use a combination of upper and lower case letters, numbers and symbols, and are not reused with any other service) with your account to avoid unauthorized use. Please let us know immediately if you think your account's security has been compromised so we can help; we are not liable for any losses of any kind caused by any unauthorized use of your account.

ii) WHAT CONTROL DO I HAVE OVER MY USE OF THE SERVICES?

You may control your profile and how you interact with the Services by changing the settings in your [settings page](#). By providing your email address to us you consent to our using the email address to send you Services-related notices, including any required legal notices and other messages, such as additions or changes to the Services and/or notices of product offers. You may opt out or change your preferences in your [settings page](#). While we need your email address to send you important Services-related notices, you can always ask us to stop sending you certain marketing messages. Opting out may prevent you from receiving email messages regarding updates, improvements, or offers.

iii) RESTRICTED USES

the Services in any medium, including but not limited to by any automated or non-automated “scraping”; (ii) use any automated system, including but not limited to “robots,” “spiders,” “offline readers,” etc., to access the Services in a manner that sends more request messages to the Clever servers than a human can reasonably produce in the same period of time by using a conventional online web browser; (iii) transmit spam, chain letters, or other unsolicited email; (iv) attempt to interfere with, compromise the system integrity or security or decipher any transmissions to or from the servers running the Services; (v) take any action that imposes, or may impose an unreasonable or disproportionately large load on our infrastructure; (vi) transmit any malicious software agents through the Services; (vii) collect or harvest any third-party personally identifiable information, including account names or Student Data (as defined below), from the Services; (viii) use the Services for any commercial solicitation purposes; (ix) impersonate another person or otherwise misrepresenting your affiliation with a person or entity, conducting fraud, hiding or attempting to hide your identity; (x) interfere with the proper working of the Services; (xi) access any content on the Services through any technology or means other than those provided or authorized by the Services; or (xii) bypass the measures we use to prevent or restrict access to the Services, including but not limited to features that prevent or restrict use or copying of any content or enforce limitations on use of the Services or related content.

We continually update our Services to offer the best possible product. While we plan to continue to offer and improve our Services, we may, without prior notice, change, cancel, create usage limits for, or permanently or temporarily stop offering or allowing you access to the Services generally (“Service Changes”). While we’ll try to give you advance notice of Service Changes that will adversely affect you, this might not be practical or possible and we retain the right to make Service Changes without notice and liability for any reason. If this Agreement ends you continue to be bound by it in any interactions you may have with the Services.

You are fully responsible for your interactions with other Users, and we have no liability for your interactions with any other Users, or for any User’s actions or inactions with respect to you.

iv) ADDITIONAL TERMS APPLICABLE TO OUR APP

To use any App you must have a mobile device that is compatible with the App. Company does not warrant that the App will be compatible with your mobile device. You may use mobile data in connection with the App and may incur additional charges from your wireless provider for these services. You agree that you are solely responsible for any such charges. Company hereby grants you a non-exclusive, non-transferable, revocable license to use a compiled code copy of the App for one Company User Account on one mobile device owned or leased solely by you, for your personal use. You may not: (i) modify, disassemble, decompile or reverse engineer the App, except to the extent that such restriction is expressly prohibited by law; (ii) rent, lease, loan, resell, sublicense, distribute or otherwise transfer the App to any third party or use the App to provide time sharing or similar services for any third party; (iii) make any copies

through the App, or features that enforce limitations on use of the App, or (v) delete the copyright and other proprietary rights notices on the App. You acknowledge that Company may from time to time issue upgraded versions of the App, and may automatically electronically upgrade the version of the App that you are using on your mobile device. You consent to such automatic upgrading on your mobile device, and agree that the terms and conditions of this Agreement will apply to all such upgrades. Any third-party code that may be incorporated in the App is covered by the applicable open source or third-party license EULA, if any, authorizing use of such code. The foregoing license grant is not a sale of the App or any copy thereof, and Company or its third-party partners or suppliers retain all right, title, and interest in the App (and any copy thereof). Any attempt by you to transfer any of the rights, duties or obligations hereunder, except as expressly provided for in this Agreement, is void. Company reserves all rights not expressly granted under this Agreement. If the App is being acquired on behalf of the United States Government, then the following provision applies. The App will be deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, reproduction, release, performance, display or disclosure of the Services and any accompanying documentation by the U.S. Government will be governed solely by these Terms of Service and is prohibited except to the extent expressly permitted by these Terms of Service. The App originates in the United States, and is subject to United States export laws and regulations. The App may not be exported or re-exported to certain countries or those persons or entities prohibited from receiving exports from the United States. In addition, the App may be subject to the import and export laws of other countries. You agree to comply with all United States and foreign laws related to use of the App and the Services.

The following applies to any App you acquire from the Apple App Store ("Apple-Sourced Software"): You acknowledge and agree that this Agreement is solely between you and Company, not Apple, Inc. ("Apple") and that Apple has no responsibility for the Apple-Sourced Software or content thereof. Your use of the Apple-Sourced Software must comply with the App Store Terms of Service. You acknowledge that Apple has no obligation whatsoever to furnish any maintenance and support services with respect to the Apple-Sourced Software. In the event of any failure of the Apple-Sourced Software to conform to any applicable warranty, you may notify Apple, and Apple will refund the purchase price for the Apple-Sourced Software to you; to the maximum extent permitted by applicable law, Apple will have no other warranty obligation whatsoever with respect to the Apple-Sourced Software, and any other claims, losses, liabilities, damages, costs or expenses attributable to any failure to conform to any warranty will be solely governed by this Agreement and any law applicable to Company as provider of the software. You acknowledge that Apple is not responsible for addressing any claims of you or any third party relating to the Apple-Sourced Software or your possession and/or use of the Apple-Sourced Software, including, but not limited to: (i) product liability claims; (ii) any claim that the Apple-Sourced Software fails to conform to any applicable legal or

as provider of the Software. You acknowledge that, in the event of any third-party claim that the Apple-Sourced Software or your possession and use of that Apple-Sourced Software infringes that third party's intellectual property rights, Company, not Apple, will be solely responsible for the investigation, defense, settlement and discharge of any such intellectual property infringement claim to the extent required by this Agreement. You and Company acknowledge and agree that Apple, and Apple's subsidiaries, are third-party beneficiaries of this Agreement as relates to your license of the Apple-Sourced Software, and that, upon your acceptance of the terms and conditions of this Agreement, Apple will have the right (and will be deemed to have accepted the right) to enforce this Agreement as relates to your license of the Apple-Sourced Software against you as a third-party beneficiary thereof.

SECTION 2. RIGHTS IN OUR CONTENT

"Student Data" is any information (in any format) that is directly related to any identifiable current or former student that is maintained by a School, and may include "educational records" as defined by the Family Educational Rights and Privacy Act ("FERPA") that Schools provide to us. While we may need to access Student Data to provide the Services to you, Schools own the Student Data and remain responsible for it. Our [Additional Terms of Use for Schools](#), [Additional Terms of Use for Developers](#), and [Privacy Policy](#) provide more detail around how we handle Student Data.

"Intellectual Property Rights" means all worldwide patent rights, copyright rights, moral rights, rights of publicity, trademark, trade dress and service mark rights, goodwill, trade secret rights and other intellectual property rights as may now exist or hereafter come into existence, and all related applications and registrations, renewals and extensions.

Except for Student Data or the applications made available by Developers, the Services and all materials made available to you in connection with them, including, but not limited to, software, images, text, graphics, illustrations, logos, patents, trademarks, service marks, copyrights, photographs, audio, videos, music, and any content belonging to other Users (the "Clever Content"), and all related Intellectual Property Rights, are the exclusive property of Clever and its licensors. Except as specified in this Agreement, nothing may be deemed to create a license in or under any such Intellectual Property Rights, and you agree not to sell, license, rent, modify, distribute, copy, reproduce, transmit, publicly display, publicly perform, publish, adapt, edit or create derivative works from any Clever Content. *To be clear: any use of the Clever Content for a purpose not expressly permitted by this Agreement is strictly prohibited.*

If you send us ideas or comments about our Services, you agree that we may freely use or reference those ideas and comments and we do not owe you any payment or have any other obligation of any kind for such ideas or comments.

SECTION 3. GENERAL LEGAL TERMS

information associated with your account (“Clever Data”). The data elements we collect and use to create Clever Data depends on your SIS type and the applications you are working with. You can find the data elements used by each application by going to your dashboard.

Clever Data is licensed to you for your use on a limited basis, and is governed solely by the terms of this Agreement and available for distribution only at our sole discretion. Clever owns the account you use to access the Services along with any rights of access or rights to data stored by or on behalf of Clever on Clever servers (except with respect to any Student Data that we may be storing for you), including but not limited to any data representing any or all of your Clever Data. Clever has the right to manage, control and even eliminate Clever Data, except that Clever may only use Student Data as specifically permitted by this Agreement.

This next sentence is in all caps because it’s important: YOU UNDERSTAND AND AGREE THAT ANY DATA, ACCOUNT HISTORY AND ACCOUNT CONTENT RESIDING ON CLEVER’S SERVERS MAY BE DELETED AT ANY TIME FOR ANY REASON IN CLEVER’S SOLE DISCRETION, WITH OR WITHOUT NOTICE AND WITH NO LIABILITY OF ANY KIND. WE DO NOT PROVIDE OR GUARANTEE, AND EXPRESSLY DISCLAIM, ANY VALUE, CASH OR OTHERWISE, ATTRIBUTED TO ANY DATA RESIDING ON CLEVER’S SERVERS. IF YOU’RE A SCHOOL, YOU SHOULD BE ABSOLUTELY SURE TO KEEP SECURE COPIES OF STUDENT DATA IN YOUR STUDENT INFORMATION SYSTEM (“SIS”) OR IN OTHER SECURE STORAGE. YOU SHOULD NOT RELY ON US TO PROVIDE COPIES OF OR ACCESS TO YOUR STUDENT DATA.

ii) PRIVACY AND SECURITY

We take very seriously the privacy of our users, including schools, teachers, parents, and students. By using the Services you consent to the collection, use and disclosure of your information (including but not limited to Student Data) as set forth in our [Privacy Policy](#) and, if you’re a School, in the [Additional Terms of Use for Schools](#), and to have your information (including but not limited to Student Data) collected, used, transferred to and processed in the United States pursuant to our [Privacy Policy](#).

iii) THIRD-PARTY SERVICES

Our website may contain links to third-party websites, services (including but not limited to applications made available by Developers), or other materials or information that are not owned or controlled by us. Keep in mind that we do not endorse or assume any responsibility for any third-party sites, information, materials, products, or services (including but not limited to applications made available by Developers). If you access a third party website or application made available by Developers from the Services, you understand that you do so at your own risk, and you understand that this Agreement, the [Additional Terms of Use for Schools](#), [Additional Terms of Use for Developers](#), and our [Privacy Policy](#) do not apply to your use of those sites or services—those sites and services have their own applicable terms and policies.

policies) are only between you and such Developers. We are not responsible for any loss or damage of any sort relating to your dealings with such Developers.

iv) INDEMNITY

You agree to defend, indemnify and hold harmless Clever and its subsidiaries, agents, licensors, managers, and other affiliated companies, and their employees, contractors, agents, officers and directors, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the Services, including any data or content transmitted or received by you; (ii) your violation of any term of this Agreement, including but not limited to your breach of any of the representations and warranties; (iii) your violation of any third-party right, including but not limited to any right of privacy or Intellectual Property Rights; (iv) your violation of any applicable law, rule or regulation, including but not limited to FERPA, the Protection of Pupil Rights Amendment ("PPRA"), and the Children's Online Privacy and Protection Act ("COPPA"); (v) any content or information that is submitted via your account; or (vi) any other party's access and use of the Services with your unique username, password or other appropriate security code.

v) WARRANTY DISCLAIMER

These next few sections are surrounded by stars so we can be sure we have your attention (conspicuous code). Formally, this section was in capital letters, but that makes this important information even more difficult to read. Again, please feel free to contact us by visiting our [Help Center](#) if any of this is unclear or if you have any questions about what these sections mean.

*** The services is provided on an "as is" and "as available" basis. Use of the services is at your own risk. To the maximum extent permitted by applicable law, the services is provided without warranties of any kind, whether express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Without limiting the foregoing, Clever, its subsidiaries, its affiliates, and its licensors do not warrant that the content is accurate, reliable or correct; that the services will meet your requirements; that the services will be available at any particular time or location, uninterrupted; that any defects or errors will be corrected; or that the services is free of viruses or other harmful components. Any content downloaded or otherwise obtained through the use of the services is downloaded at your own risk and you will be solely responsible for any damage to your computer system or loss of data that results from such download or your use of the services. ***

*** We do not warrant, endorse, guarantee, or assume responsibility for any product or services advertised or offered by a third party through the services or any hyperlinked website or services (including without limitation applications), and we will not be a party to or in any way monitor any transaction between you and third-party providers of products or services (including without limitation developers). ***

vi) LIMITATION OF LIABILITY

*** To the maximum extent permitted by applicable law, in no event shall Clever, its affiliates, agents, directors, employees, suppliers or licensors be liable for any indirect, punitive, incidental, special, consequential or exemplary damages, including without limitation damages for loss of profits, goodwill, use, data or other intangible losses, that result from the use of, or inability to use, this services. Under no circumstances will Clever be responsible for any damage, loss or injury resulting from hacking, tampering or other unauthorized access or use of the services or your account or the information contained therein. ***

*** To the maximum extent permitted by applicable law, Clever assumes no liability or responsibility for any (i) errors, mistakes, or inaccuracies of content; (ii) personal injury or property damage, of any nature whatsoever, resulting from your access to or use of our services; (iii) any unauthorized access to or use of our secure servers and/or any and all personal information stored therein; (iv) any interruption or cessation of transmission to or from the services; (v) any malicious software agents that may be transmitted to or through our services by any third party; (vi) any errors or omissions in any content or for any loss or damage incurred as a result of the use of any content posted, emailed, transmitted, or otherwise made available through the services; and/or (vii) content you create or the defamatory, offensive, or illegal conduct of any third party. In no event shall Clever, its affiliates, agents, directors, employees, suppliers, or licensors be liable to you for any claims, proceedings, liabilities, obligations, damages, losses or costs in an amount exceeding the amount you paid to Clever hereunder or \$100.00, whichever is greater. ***

*** This limitation of liability section applies whether the alleged liability is based on contract, tort, negligence, strict liability, or any other basis, even if Clever has been advised of the possibility of such damage. The foregoing limitation of liability shall apply to the fullest extent permitted by law in the applicable jurisdiction. ***

The Services are controlled and operated from US-based facilities, and we make no representations that they're appropriate or available for use in other locations. If you access or use the Services from other jurisdictions, you understand that you're entirely responsible for compliance with all applicable United States and local laws and regulations, including but not limited to export and import regulations. Because we have to say this, you may not use the Services if you are a resident of a country embargoed by the United States, or are a foreign person or entity blocked or denied by the United States government.

vii) GOVERNING LAW

You agree that: (i) the Services will be deemed solely based in California; and (ii) the Services will be deemed passive services that do not give rise to personal jurisdiction over us, either specific or general, in jurisdictions other than California. This Agreement will be governed by

does not apply. You agree to submit to the personal jurisdiction of the federal and state courts located in Santa Clara County, California for any actions related to this Agreement.

viii) SEVERABILITY AND WAIVER

This Agreement, and any rights and licenses granted hereunder, may not be transferred or assigned by you, but may be assigned by us in accordance with the terms of our [Privacy Policy](#). This Agreement, together with any amendments and any additional agreements you may enter into with Clever in connection with the Services including other agreements referenced herein, constitute the entire agreement between you and Clever concerning the Services. If any provision of this Agreement is deemed invalid by a court of competent jurisdiction, the invalidity of such provision will not affect the validity of the remaining provisions of this Agreement, which will remain in full force and effect. No waiver of any term of this Agreement will be deemed a further or continuing waiver of such term or any other term, and Clever's failure to assert any right or provision under this Agreement will not constitute a waiver of such right or provision. If access to the Services is licensed to the United States government or any agency thereof, then the Services will be deemed to be "commercial computer software" and "commercial computer software documentation," pursuant to DFARS Section 227.7202 and FAR Section 12.212, respectively, as applicable. Any use, reproduction, release, performance, display, or disclosure of the Services and any accompanying documentation by the U.S. Government will be governed solely by this Agreement and is prohibited except to the extent expressly permitted by this Agreement. Neither party will hold themselves out to be joint venturers, and neither party is authorized or empowered to act as the agent of the other.

[↑ Back to top](#)



Products

[Rostering](#)

[Single Sign-on](#)

[Clever Badges](#)

[Clever Library](#)

Company

[About us](#)

[Careers](#)

[Engineering](#)

[Blog](#)

Trust

[Trust](#)

[Privacy](#)

[Security](#)

[Compliance](#)

Help

[Help center](#)

[Clever Academy](#)

[Contact](#)

© Clever Inc.

[Terms of service](#)

[Privacy Policy](#)

[Accessibility statement](#)

Clever Additional Terms of Use for Schools

Effective Date: October 11, 2019

Welcome to Clever's Additional Terms of Use for Schools (the "Additional Terms for Schools"). If you are a School, please also review our [General Terms of Use](#) and our [Privacy Policy](#). If you're not a School (as defined in the [General Terms of Use](#)), these Additional Terms for Schools do not apply to you.

Capitalized terms that are not defined below have the definitions given them in the [General Terms of Use](#).

By using the Services, you authorize us to access your SIS or receive Student Data or other information via SIS, Secure File Transfer Protocol ("SFTP"), or any other secure transfer method to provide you software integration services.

SECTION 1. KEEPING YOUR STUDENT DATA CONFIDENTIAL (THIS IS VERY IMPORTANT TO US) AND COMPLYING WITH APPLICABLE LAWS

We treat your Student Data as confidential and do not knowingly share it with third parties other than as described in Section 2(B) and in the [General Terms of Use](#) and our [Privacy Policy](#).

Both parties agree to uphold their responsibilities under the Family Educational Rights and Privacy Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), and the Children's Online Privacy and Protection Act ("COPPA"). We provide the Services under the school official exception of FERPA 34 CFR Part 99.31(a)(1). The Children's Online Privacy and Protection Act ("COPPA") requires that online service providers obtain clear and verifiable parental consent before collecting personal information from children under 13. You represent and warrant that you have the authority to provide consent on behalf of parents, for us to collect information from students for the purpose of providing the Services to you as described in these Terms before allowing children under 13 to access our Services. We recommend that all Schools provide appropriate disclosures to students and parents regarding their use of service providers such as Clever and that they provide a copy of our Privacy Policy to parents and guardians.

SECTION 2. AUTHORIZATION TO ACCESS YOUR STUDENT DATA

stored in your SIS. We will access and process Student Data only in order to provide the Services. As between us, you own all right, title and interest to all Student Data, you are (and other Schools are) solely responsible for any and all Student Data, whether provided by you, students, or others, and we do not own, control, or license Student Data, except to provide the Services.

B. THIRD PARTY ACCESS

You may designate one or more third-party Developers to securely access Student Data via our API. We will not send Student Data to a Developer unless explicitly authorized by you. You acknowledge that we are not responsible for the data practices of third party Developers, and that, as between us, you are solely responsible for the consequences of providing or transmitting Student Data to such Developers, or authorizing those Developers to access Student Data through the Services. At any time, you can revoke any Developer's ongoing access to Student Data via the API by visiting our [Help Center](#).

We provide access to Student Data only to those employees and certain trusted service providers who have a legitimate need to access such information in connection with providing the Services to you. Of course, anyone involved in the handling of Student Data will treat such data as strictly confidential and shall not redisclose such data except as necessary in order to provide the Services. We will maintain access log(s) that record all disclosures of or access to Student Data within our possession and will provide copies of those access log(s) to you on your request.

C. OTHER ACCESS

Student Data is controlled by Schools. Parents, legal guardians, and students can ask for their Student Data via their Schools. If there are any changes that need to be made in Clever, the district will upload the new Student Data to Clever.

SECTION 3. HOW WE USE YOUR STUDENT DATA

A. IN GENERAL

By submitting Student Data or other information to us, whether via the Services or otherwise, you expressly grant, and you represent and warrant that you have all rights necessary to grant, to us a non-exclusive, royalty-free, worldwide license during the term of these Additional Terms for Schools and our [General Terms of Use](#) to use, transmit, distribute, modify, reproduce, display, and store the Student Data only for the purposes of: (i) providing the Services as contemplated in these Additional Terms for Schools and our [General Terms of Use](#), and (ii) enforcing our rights under these Additional Terms for Schools and our [General Terms of Use](#). Subject to the Paragraph B below, we will not use the Student Data for any purpose except as

B. ANONYMIZED DATA

You agree that we may collect and use data derived from Student Data, including data about any Users' access and use of the Services, that has been anonymized, aggregated, or otherwise de-identified such that the data cannot reasonably identify a particular student, User, or School. We may use such data to operate, analyze, improve or market our Services or to develop other educational sites, services or applications. If we share or publicly disclose information (e.g., in marketing materials) that is derived from Student Data, that data will be aggregated or anonymized to reasonably avoid identification of a specific School or individual student. For example, we may (i) track the number of School administrators on an anonymized aggregate basis as part of our marketing efforts to publicize the total number of Users of the Services, and (ii) analyze aggregated usage patterns for product development efforts. You further agree that we may use, store, transmit, distribute, modify, copy, display, sublicense, and create derivative works of the anonymized, aggregated Student Data even after this Agreement has expired or been terminated.

SECTION 4. DELETING STUDENT DATA AND TERMINATING YOUR ACCESS TO THE SERVICES

A. DELETING STUDENT DATA

You may request in writing that we delete any of your Student Data (except as provided for the Section 3(B) above) in our possession at any time. We will comply with your request in a commercially reasonable time not to exceed ten (10) business days. If you grant access to Student Data to a Developer and subsequently need that data deleted, you need to request such deletion directly from that Developer.

B. TERMINATING YOUR ACCESS TO THE SERVICES

Schools may, at any time and for any or no reason, terminate these Additional Terms for Schools and our [General Terms of Use](#) by providing written notice by visiting our [Help Center](#), except that provisions that by their nature should survive termination will survive termination, such as provisions relating to warranty disclaimers, limitations of liability, indemnities, and governing law.

Within seventy-two (72) hours of our receipt of such notice of termination or earlier if commercially reasonable to do so, we will cease accessing your SIS. We will automatically delete or de-identify all Student Data within seventy-two (72) hours of our receipt of the termination notice, except for Student Data residing on backups or internal logs which will be removed within sixty (60) days, and will provide notice to the School when Student Data has been deleted and/or anonymized as described in Section 3(B) above. As noted above, Student Data that has previously been made available to Developers may still be in Developers'

any agreements between School and Developers. We may terminate these Additional Terms for Schools and our [General Terms of Use](#) in accordance with the [General Terms of Use](#).

SECTION 5: PRIVACY AND SECURITY

We care deeply about the privacy and security of Student Data. We maintain strict administrative, technical, and physical safeguards to protect Student Data stored in our servers, which are located in the United States. We limit access to Student Data only to those employees or service providers who have a legitimate need to access such data in the performance of their duties. All of our employees with access to Student Data are required to have passed a background check and receive annual training on how to maintain the security and confidentiality of student records.

If there is any disclosure or access to any personally identifiable Student Data by an unauthorized party (a "Security Incident"), we will promptly notify the Clever account owner of any affected Schools via email and will use reasonable efforts to cooperate with their investigations of the incident. 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, you agree that, as the owner of the Student Data, you may be responsible for the timing, content, cost, and method of any required notice and compliance with those laws. However, at the request of the School and when permissible under applicable law, Clever agrees to bear responsibility for the timing, content and method of such required notice on behalf of the Schools. In all instances, Clever will indemnify Schools for all reasonable costs associated with compliance with such notice requirements arising from a breach of the Clever Service. For clarity and without limitation, Clever will not indemnify for any notification costs arising from a breach of a third party application whose service is accessed through the Clever Service.

SECTION 6: FEES AND PAYMENT TERMS

You agree to pay all fees specified in an ordering document or an online order that is entered into between you and Clever (each, and "Order Form") on the payment schedule set forth in such Order Form. Except as otherwise specified in an Order Form, all payment obligations are non-cancelable and fees paid are non-refundable. You will provide us with either valid credit card information, a valid purchase order or alternative payment document reasonably acceptable to us. If you provide us with a credit card, then you authorize us to charge such credit card for all purchased products and services listed in the Order Form(s). Such charges will be made in advance, either annually or in accordance with any different billing frequency stated in the applicable Order Form. If the Order Form specifies that payment will be by a

due net 30 days from the invoice date. You are responsible for providing complete and accurate billing and contact information to us and notifying us of any changes to such information. If any amount owing by you under this Agreement or any other agreement is 30 or more days overdue, then we may, without limiting our other rights and remedies, suspend our Services to you until such amounts are paid in full. Prices and fees are exclusive of any federal, state, local or other taxes, which will be your responsibility, unless you provide us with proof of your tax-exempt status. Taxes, if any, will be listed separately on the invoice. Upon our request, you will provide us with a certificate or other evidence documenting your tax-exempt status.

SECTION 7. QUESTIONS

We here at Clever hope that you will have the best possible experience when using our Services. If you have any questions or concerns about our Services or anything in our [General Terms of Use](#), these Additional Terms for Schools, or our [Privacy Policy](#), please don't hesitate to contact us by visiting our [Help Center](#) and we'll do our best to promptly respond to you.

Thanks for reading!

↑ [Back to top](#)



Products

- Rostering
- Single Sign-on
- Clever Badges
- Clever Library
- Pricing

Company

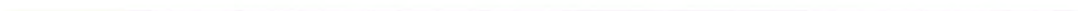
- About us
- Careers
- Engineering
- Blog
- News
- Events
- Contact

Trust

- Trust
- Privacy
- Security
- Compliance

Help

- Help center
- Clever Academy



Clever's Commitment to Your Privacy

Clever is a proud signatory of the [Student Data Privacy Pledge](#).

Clever ("Clever," "we," or "us") understands that privacy is tremendously important to our online visitors to our website ("Website Visitors"), to schools who use our Service ("Schools"), and to students whose information we may access on behalf of a School ("Students"). Clever provides a platform that enables Schools to securely provision the accounts with the third-party applications, that they use. As we describe below, Schools decide which data is integrated with Clever, and Schools are responsible for determining whether data is ever shared with applications through Clever. This privacy policy applies to our website <https://clever.com/> and to the Clever platform (our "Service") and describes the steps we take to protect your data.

Capitalized terms that are not defined in this Privacy Policy have the meaning given them in our [Terms of Use](#).

Click on the links below to jump to each section:

- [How We Collect and Use Information](#)
- [Sharing of Your Information](#)
- [How We Store and Protect Your Information](#)
- [Your Choices About Your Information](#)
- [Children's Privacy](#)
- [Links to Other Websites and Services](#)
- [How to Contact Us](#)
- [Jurisdiction-Specific Disclosures](#)
- [Changes to Our Privacy Policy](#)

We strive to be transparent in our data collection and use practices. This is the type of personal information we may collect.

1. HOW WE COLLECT AND USE INFORMATION

We collect the following types of information:

name, school name, school district, school email address and/or account name and password, phone number, message content, and information relating to the School's information systems. We may also retain information provided by a School if the School sends us a message, posts content to our website or through our Service, or responds to emails or surveys. Once a School begins using the Clever Service, we will collect content and information provided by the School through the School's use of the Service and we will keep records of activities related to the Service. We use this information to operate, maintain, and provide to the features and functionality of the Service, to analyze and improve our Service offerings and functionality, and to communicate with our Schools and website visitors.

Student Data: Through the course of providing its Service to a School, Clever may have access to personally identifiable information about students ("Student Data") that is provided by the School, by the parent or guardian, or by the Student. Depending on the Service selected by the School, a School may authorize Clever to receive Student Data from the learning application(s) used by the School. Clever has access to Student Data only as requested by the School and only for the purposes of performing Services on the School's behalf. The type of Student Data we collect will depend on how the School uses the Service and the learning applications which the School connects through the Service. In many instances, Clever receives Student Data only from the School and never interacts with the Student directly. In some instances, depending on the level of Clever's Service selected by the School, the Schools may allow Students to log into the Clever Service to access third party applications that have been authorized by the School. In that instance, the School provides each student with login credentials and confirms that it has obtained appropriate parental consents, as needed, before the student is permitted to access the Service.

Badges: As an alternative to a user name and password login, a School may choose to use the Clever Badge to authenticate Student users. The Clever Badge is a QR code provided by the School to the Student (usually in the form of a laminated card or paper print-out) which recognizes a user's Clever account when the Badge is read by the camera on a Chromebook, laptop or other device. Clever does not collect or store any image collected by the device camera. The camera content is processed on the users' device and Clever only receives the tokens used for authentication. You can learn more about Clever Badges [here](#).

We consider Student Data to be confidential and do not use such data for any purpose other than to provide the services on the School's behalf, in accordance with contractual agreements with the School. Our collection, use, and disclosure of Student Data is governed by our Terms of Use, our Additional Terms of Use for Schools, and/or any other agreement with the School, by the provision of the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and applicable state laws which relate to the collection of Student Data. If you are a Student or parent, please contact your School if you have questions about the School's use of technology service providers like Clever.

we collect and use the personal information of children under 13.

Information collected through technology: Like most websites and online services, we and our third party partners automatically collect certain types of usage information when you visit our Services, read our emails, or otherwise engage with us. We typically collect this information through a variety of tracking technologies, including cookies, web beacons, file information and similar technology (collectively, "tracking technologies"). For example, we collect information about your device and its software, such as your IP address, browser type, Internet service provider, platform type, device type, operating system, date and time stamp, a unique ID that allows us to uniquely identify your browser, mobile device or your account, and other such information. We also collect information about the way you use our Service, for example, the site from which you came and the site to which you are going when you leave our website, the pages you visit, the links you click, how frequently you access the Service, whether you open emails or click the links contained in emails, whether you access the Service from multiple devices, and other actions you take on the Service. When you access our Service from a mobile device, we may collect unique identification numbers associated with your device or our mobile application, mobile carrier, device type, model and manufacturer, mobile device operating system brand and model. We may be able to determine your approximate location by analyzing other information, a device's location by analyzing other information, like an IP address to associate a user with their School. We may also collect analytics data, or use third-party analytics tools, to help us measure traffic and usage trends for the Service. Although we do our best to honor the privacy preferences of our visitors, we are not able to respond to Do Not Track signals from your browser at this time.

Cookies and related technology allow us to provide you with a better user experience. For example, we may use the data collected through cookies to: (a) remember information so that a user will not have to re-enter it during subsequent visits; (b) provide custom, personalized content and information; (c) to identify you across multiple devices; (d) to provide and monitor the effectiveness of our Service; (e) monitor aggregate metrics such as total number of visitors, traffic, and usage on our website and our Service; (f) diagnose or fix technology problems; (g) help users efficiently access information after signing in, and (h) otherwise to plan for and enhance our Service

If you would prefer not to accept cookies, most browsers will allow you to: (i) change your browser settings to notify you when you receive a cookie, which lets you choose whether or not to accept it; (ii) disable existing cookies; or (iii) set your browser to automatically reject cookies. Please note that doing so may negatively impact your experience using the Service, as some features and services on our Service may not work properly. Depending on your mobile device and operating system, you may not be able to delete or block all cookies. You may also set your e-mail options to prevent the automatic downloading of images that may contain technologies

Third Party Tracking: We do not permit third party advertising networks to collect information about your use of our website and Service over time and across websites for the purpose of serving targeted advertising and we will never use Student Data for targeted advertising.

Student privacy is very important to us. Student Data is used only for educational purposes at the direction of the School.

2. HOW WE SHARE YOUR INFORMATION

Clever only shares personal information in a few limited circumstances, described below. We do not rent or sell information for marketing purposes and we will never share or sell Student Data with third parties for marketing purposes.

Who we may share information with:

- We share information within the Service as needed to perform the Service and/or at the direction of the School. For example, information including Student Data, will be shared between and among authorized School users such as teachers and School administrators. This sharing will depend on the settings and functionality selected by the School.
- We may share information with our trusted third party service providers who perform technology services on our behalf (e.g. web hosting and analytics services), but strictly for the purpose of carrying out their work for us. Contractors and service providers who may have access to Student Data in the course of performing their services are subject to confidentiality and data security requirements.
- We may be required to share information with law enforcement or other third parties when compelled to do so by court order or other legal process, to comply with statutes or regulations, to enforce our [Terms of Use](#), or if we believe in good faith that the disclosure is necessary to protect the rights, property or personal safety of our users.
- We may share information in an aggregated and/or anonymous form that does not reasonably identify an individual or School. For example, we may use and share aggregate or anonymized data to study and improve our Service, user functionality, and product offerings.

In the event of a change of control: If we sell, divest or transfer our business, we will not transfer personal information of our customers unless the new owner intends to maintain and provide the Service as a going concern, and provided that the new owner has agreed to data privacy standards no less stringent than our own. In such case we will provide you with notice and an opportunity to opt-out of the transfer of personally identifiable Student Data.

so on behalf of the School. Some elements of our Service enable Schools to interact with parents, students, teachers and third party applications, for the benefit of the student's education. Clever does not facilitate the sharing of any Student Data with third parties on the Service except on behalf of the School after the School has authorized a third party or application to access Student Data through the Service. Please remember that this Privacy Policy applies to the Clever Services, and not other services or third party applications, which may have their own privacy policies. Schools should carefully read the privacy practices of each third party application before agreeing to engage with the application through the Service.

We store our data in the United States and we take strong measures to keep data safe and secure.

3. HOW WE STORE AND PROTECT YOUR INFORMATION

Storage and processing: Any information collected through the Service is stored and processed in the United States. If you use our Service outside of the United States, you consent to have your data transferred to the United States.

Keeping information safe: Clever maintains strict administrative, technical and physical procedures to protect information stored in our servers, which are located in the United States. Access to information is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include but are not limited to data encryption, firewalls, and physical access controls to building and files.

Unauthorized disclosure: If there is any disclosure or access to any personally identifiable Student Data by an unauthorized party, we will promptly notify the affected School(s) and will use reasonable efforts to cooperate with their investigation of the incident.

Questions about data? Here are your options.

4. YOUR CHOICES ABOUT YOUR INFORMATION

Account information and settings: Schools may update account information and modify Services by signing into the administrator account. Schools and other website visitors can opt-out of receiving promotional email from us by clicking on the "unsubscribe" feature at the bottom of each email. Sorry, you cannot unsubscribe from Service-related messaging.

If you have any questions about reviewing or modifying account information, contact us directly by visiting our [Help Center](#).

contact your School directly.

How long we keep User Content: Following termination or deactivation of a School account, Clever may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes, but any and all Student Data associated with the School will be deleted promptly. We may maintain anonymized or aggregated data, including usage data, for analytics purposes. If you have any questions about data retention or deletion, please contact us by visiting our [Help Center](#).

We do not collect any information from students without consent.

5. CHILDREN'S PRIVACY

Clever does not knowingly collect any information from children under the age of 13 unless and until the School has obtained appropriate parental consent for the student to use the Service. Because Clever collects and uses Student Data at the direction of and under the control of a School, Clever relies on each School to provide appropriate notice to parents of the School's use of third party service providers such as Clever, and for the Schools to provide consent, if necessary, and authorization for Clever to collect Student Data, as permitted by the Children's Online Privacy Protection Act (COPPA). Please contact us at urgent@clever.com if you believe we have inadvertently collected personal information of a child under 13 without proper consent so that we may delete such data as soon as possible.

6. LINKS TO OTHER WEB SITES AND SERVICES

We are not responsible for the practices employed by websites, applications or services linked to or from our Service. We recommend that the School review the privacy policies of other applications before authorizing a third party to access data through the Service.

7. HOW TO CONTACT US

If you have any questions about this Privacy Policy or the Service, we recommend contacting us by visiting our [Help Center](#).

Additionally, Clever can be reached:

- By Email: trust@clever.com
- By Mail: Clever Inc, ATTN: Dan Carroll, 1263 Mission St, San Francisco CA 94103

dedicated consumer complaint department at: coppaprivacy@ikeepssafe.org

If a Student contacts Clever with a question about our Service, we will collect personal information from that Student only as necessary to respond to the Student's request and direct the Student to contact the Student's School, and we will then delete or anonymize the personal data of the Student after providing our response.

8. JURISDICTION-SPECIFIC DISCLOSURES

We may be required by law to provide additional privacy disclosures, depending on the jurisdiction in which you reside. Please refer below for disclosures that may be applicable to you:

- *California.* If you are a California resident, please [click here](#) for additional California-specific privacy disclosures.
- *Nevada.* Chapter 603A of the Nevada Revised Statutes permits a Nevada resident to opt out of future sales of certain covered information that a website operator has collected or will collect about the Nevada resident. At this time, we do not engage in data "sales" as defined by the Nevada law. However, if you would like to submit a request to opt-out of future sales (if any), please contact us directly by visiting our [Help Center](#). You can also email us at support@clever.com with the with the subject line "Nevada opt-out."

9. CHANGES TO OUR PRIVACY POLICY

Clever may modify or update this Privacy Policy from time to time so you should review this page periodically. [Click here](#) to see all changes to this Privacy Policy. If we change the policy in a material manner, for example if we seek to use personal information in a materially different way than we had previously, we will provide at least 30 days notice to the Schools so that you have sufficient time to evaluate the change in practice. Of course, you can always opt-out by deleting your account before the changes take effect.

This privacy policy was last modified on December 19, 2019. Effective Date: January 1, 2020

[Rostering](#)[About us](#)[Trust](#)[Help center](#)[Single Sign-on](#)[Careers](#)[Privacy](#)[Clever Academy](#)[Clever Badges](#)[Engineering](#)[Security](#)[Clever Library](#)[Blog](#)[Compliance](#)[Pricing](#)[News](#)[Events](#)[Contact](#)

Privacy Disclosures for California Residents

This Privacy Notice for California Residents (“CA Notice”) supplements the Clever Privacy Policy as well as any other agreement you may have with us. Any terms we use in this CA Notice that aren’t defined will have the meaning we provide in the Privacy Policy or other agreements.

California law requires us to disclose certain information regarding the categories of personal information we collect. For purposes of this CA Notice, “personal information” has the meaning provided by the California Consumer Privacy Act (the “CCPA”) and does not include information that is publicly available, that is deidentified or aggregated such that it is not capable of being associated with us, or that is excluded from the CCPA’s scope, such as personal information covered by certain sector-specific privacy laws, such as the HIPAA, the FCRA, GLBA or the Driver’s Privacy Protection Act of 1994. This CA Notice does not apply to information relating to our employees, contractors, or other personnel.

A note about Student Data. Clever provides the Services to Schools as a “School Official” under FERPA. That means that we collect, retain, use and disclose Student Data only for or on behalf of a School customer for the purposes of providing the Services specified in our agreement with the School, and for no other commercial purpose. Under the CCPA, we collect, retain, use and disclose Student Data as a service provider to our School customers and **this CA Notice does not describe our practices with regard to Student Data or any other personal information we process as a service provider.** If you have a question or would like to exercise your California consumer rights to knowledge, access or deletion, please contact your School directly.

Collection and use of personal information. We collect personal information from and about you for a variety of purposes. For example, we use personal information to respond to your requests, engage with you as a customer, developer or other vendor, and provide our Services to you or receive Services from you; for marketing and advertising purposes; to monitor, improve, and develop our products and Services; and to protect the security and integrity of our business, comply with legal requirements and obligations; for our business and operational purposes; and as otherwise permitted or required by law.

The type of personal information we collect will depend on how you engage with us (for example, as a customer or potential customer, as a Developer, or as a website visitor). In the last 12 months, we have collected the following categories of personal information:

- Professional and educational information, if you apply for a job with us through our website;
- Commercial information, such as a history of our Services purchased, obtained or considered;
- Internet/Network information, such as device information, logs and analytics data;
- Geolocation data, such as precise location data from your device or generated based on your IP address; and
- Inferences about your interests and preferences, generated from your use of our sites.

We collect this information directly from you, from our business partners and affiliates, from your browser or device when you visit our websites, or from third parties that you permit to share information with us.

Disclosure of Personal Information. We share personal information with third parties for business purposes or we may sell your personal information to third parties, subject to your right to opt out of those sales (see **Your Rights and Choices** below). The categories of third parties to whom we disclose your personal information may include: (i) our service providers and advisors, (ii) vendors who assist us with marketing and advertising our services; (iii) analytics providers; (iv) third parties with your consent or at your direction, or with whom you interact through our Service.

When we disclose your personal information to our service providers, vendors or other third parties that process the information on our behalf, we have entered into a written contract that includes terms substantially similar to this notice and we will remain liable for any breach of this notice that is caused by the acts or omissions of our service providers.

We do not sell your personal information for monetary or other valuable consideration.

Your Rights and Choices. As a California resident, you may be able to request to exercise the following rights:

- The Right to Know any or all of the following information relating to your personal information we have collected and disclosed in the last 12 months, upon verification of your identity:
 - The specific pieces of personal information we have collected about you;
 - The categories of personal information we have collected about you;
 - The categories of sources of the personal information;
 - The categories of personal information that we have disclosed to third parties for a business purpose, and the categories of recipients to whom this information was disclosed;
 - The categories of personal information we have sold and the categories of third parties to whom the information was sold; and

subject to certain exceptions.

- The Right to Opt Out of Personal Information Sales to third parties now or in the future.

You also have the right to be free of discrimination for exercising these rights. However, please note that if the exercise of these rights limits our ability to process personal information (such as in the case of a deletion request), we may no longer be able to provide you our products and services or engage with you in the same manner.

To Submit your California Consumer Rights Requests. You may submit a request to exercise your California Consumer Rights through one of the mechanisms described below. We will need to verify your identity before processing your request, which may require us to request additional personal information from you or require you to log into your account, if you have one. In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or as permitted by law.

- To exercise your Right to Know, please use the [consumer rights form](#) and email us at support@clever.com
- To exercise your Right to Request Deletion, please use the [consumer rights form](#) and email us at support@clever.com

[↑ Back to top](#)



Products

- Rostering
- Single Sign-on
- Clever Badges
- Clever Library
- Pricing

Company

- About us
- Careers
- Engineering
- Blog
- News
- Events

Trust

- Trust
- Privacy
- Security
- Compliance

Help

- Help center
- Clever Academy

