LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: Information Protection Policy

NUMBER: BUL-1077.2

ISSUER: David Holmquist, General Counsel
Office of the General Counsel

DATE: July 18, 2017

ROUTING
All Employees
All Schools

PURPOSE: It is the policy of the Los Angeles Unified School District (LAUSD) to protect sensitive information pertaining to students, employees and District operations. The purpose of this bulletin is to define the requirements for maintaining the security of information within the District. As a public institution, much of the information possessed by the District is a matter of public record. However, there are types of information that require care and sensitivity in handling, such as student education records, employee personnel records, and health care records. This bulletin also addresses data ownership and the responsibilities of data owners.

Note: Restrictions on information release are increasing, new laws to protect privacy are constantly being passed, and older ones are strengthened. This policy is a general Information Protection Policy and is not intended to cover all laws concerning privacy rights and the handling of sensitive information. If your work includes sensitive information it is essential to keep up with the laws and requirements that affect what you do.

MAJOR CHANGES: Recently enacted laws pertaining to student data privacy have been added and student data protection procedures have been clarified.

GUIDELINES: The following guidelines apply.

Background Information

Different types of information within the District have different levels of sensitivity. Some information, like that available on the District's website, is considered freely accessible public information. Other types of information are protected by state and/or federal law.

Sensitivity Levels

District Information falls into one of four basic security levels:

1. Public Information: Information published on the District's website or in other District publications. For example, the District collects data on the

number of students currently enrolled District-wide and that information is available on the District's website. This is an example of Public Information.

2. Non-published Public Information: Information that exists in the form requested, but has not been published. Summarized student attendance data is not published but is public information. This is an example of Non-published Public Information. Such information is subject to disclosure under the California Public Records Act.

3. Non-Public Information: Information that by policy the District prevents from publication. For example, prior to an award under a Request for Proposal solicitation and/or a recommendation to the Board the District will not reveal the results of evaluations of vendor proposals. This would be an example of Non-Public Information.

4. Protected Information: Information that is protected by specific laws. For example, student records, student and employee health records, and social security numbers, are each covered by specific privacy laws and rules. See Attachment A - LAUSD FERPA Policy, Attachment B - LAUSD HIPAA Policy Regarding Student Information, and Attachment C - LAUSD Employee Record Policy for more information about these types of protected information.

Information in categories 3 and 4 should not be released without the approval of the appropriate office. This usually involves input from the Office of the General Counsel along with other offices such as the Office of Data and Accountability and Procurement Services Division.

While the release of personally identifiable information from the education records of a student usually requires parental consent, there are various exceptions to the consent requirement – two of which are frequently used by the District. These exceptions apply when the District contracts with an outside vendor to perform services usually performed by a District employee or to conduct studies to improve instruction. FERPA and the California Education Code require that the District enter into an agreement than governs the disclosure of student records. Examples of such agreements are included as Attachments A-3 and A-4 to the FERPA Policy.

Employees of the District often need access to sensitive information to carry out their jobs. However, it is important to follow appropriate guidelines whenever information is transferred inside or outside the District. In general, all information needs to be handled in a secure way that protects privacy.

Public Records Act Requests

Members of the public or press may seek District records under the California "Public Records Act," California Government Code section 6250, et seq. Whatever the sensitivity level of the information, if a request for information has been made pursuant to the Public Records Act, that request should be directed to:

California Public Records Act Requests
Office of the General Counsel
Los Angeles Unified School District
333 S. Beaudry Avenue, 24th Floor
Los Angeles, CA 90017
P: (213) 241-6601
F: (213) 241-8444
E: pra@lausd.net

Data Ownership

A data owner is the administrator, director, or supervisor of the branch or division that collects and/or uses the data on behalf of the entire District. Data owners possess responsibilities for the protection of District information or data. Regardless of the form the information is in, final decision-making authority regarding whether information is released resides with the director of the division that owns that information. Data ownership is not determined by the format in which it is requested. For example, "computerized" financial information is "owned" by the Office of the Chief Financial Officer, not the Information Technology Division. Schools are generally not considered "owners" of data for the purposes of determining the appropriateness of its release. For example, an individual student's score on a standardized test is "owned" by the Executive Director and the Office of Data and Accountability, but not by the teacher who administered the test. A listing of current data owners is included in Attachment D. The data owner will coordinate with the Office of the General Counsel, Information Technology Division (ITD), and/or the Office of Communications as necessary to determine if access will be allowed, and to provide appropriate protection.

Significant responsibility lies with the owner of the data. The fact that someone is a school district employee is not a reason in and of itself to allow that person access to all information. The data owner must evaluate if there is a legitimate reason a school district employee needs access to the information in question to do their job. If access is granted by the owner of the data, the owner must also ensure the person granted access is trained in the owner's responsibilities to protect the data. It is recommended that data owners and supervisors have individuals sign an access form stating they understand their responsibility to protect data and understand the limits of the permitted use of the data. A copy of an Information Responsibility Agreement is attached as Attachment E.

Because many types of information are now available electronically, the owner of the data must evaluate the risk of allowing electronic access to data and ensure sufficient safeguards are provided to prevent inadvertent or unauthorized access to the data. Prior to authorizing the release of information, the data owner should confer with both the Office of the General Counsel and ITD Security to evaluate their options. Information belonging to another data owner should never be released without prior approval.

Employee Responsibility

Every employee of the District must ensure the proper protection of information, whether in paper or electronic form. An employee is not to take sensitive records home nor leave them lying unprotected in the open, such as on a desk, where they can be accessed. An employee is not to convert sensitive information into an electronic format and send it unprotected through email or over the Internet. Whenever requests for access to information are made, school administrators must evaluate whether it is proper to release information by checking with the data owner for guidance. It is best to err on the side of protecting information rather than risk violating an employee's or student's rights of privacy.

Policies

The following policies apply to all District personnel. The following policies apply whether the request is for one-time access to the information or the request is for continuous access to information, such as where a requestor seeks to establish a computerized link to a database containing information.

1. If any party within or outside of the District requests Public Information (Category 1), direct the requesting party to the District website or other publication containing the information. If you do not know which specific publication contains the information, direct the requesting party to the Office of Communications at (213) 241-6766.

2. If the request for information is a formal Public Records Act request, refer it immediately to the Office of the General Counsel, Public Records Unit.

3. Requests for any other kind of information should be immediately directed to the data owner. (See Attachment D) The Data Owner will consult with the General Counsel as necessary to determine if the request can legally be fulfilled, and with ITD to determine how to fulfill the request if the information is currently or will be housed in District computer systems. If you do not know who the data owner is, please refer the requesting party to the Office of Communications, which will forward the request to the appropriate data owner.

4. Vendor Access to Information—All contracts allowing a vendor access to

any kind of information other than Public Information (Category 1) must be approved by the owner of the data that is to be provided. If vendors require access to District student information to perform their contracts then Attachment A-3 or A-4 should be used, unless those terms are included in a contract processed by Procurement Services. Vendors should be provided with only that information necessary for them to perform their contracts with the District.

5. Employee Access to Information—Not all District employees have a right to access all District information. District employee access to information should be restricted to information necessary for them to perform those duties assigned by their supervisors. Supervisors should carefully evaluate each employee's need to access particular information, and should manage access accordingly. This is a management responsibility. If you are a supervisor and are not sure whether certain employees require access, consult with the data owner before providing such access.

6. Student/External Researchers—Access to information is sometimes requested by student researchers (e.g. graduate students) or other researchers seeking to access District information. Such requests should be referred to the Office of Data and Accountability.

Violations of Policy

1. Violations of this Information Protection Policy may result in discipline, up to and including dismissal.

2. Violations of certain portions of this policy could result in a civil lawsuit for a violation of privacy rights, or prosecution by a governmental agency charged with enforcing those rights.

AUTHORITY: This policy is established to address privacy rights contained within the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act, the California Education Code, the Federal Health Information Portability and Accountability Act (HIPAA), and other Federal and State Laws.

Relevant laws enacted since the last version of this bulletin include: SB 568 "Privacy Rights for California Minors in the Digital World" (California Business and Professions Code section 22850, et seq.); SB 1177 "Student Online Personal Information Protection Act" (Business and Professions Code section 22584 et seq.); and AB 1584 pertaining to "Contracts with Third Parties for Digital Storage and Management of Pupil Records" (Education Code section 49073.1).

ATTACHMENTS: LAUSD FERPA POLICY
A-1. DISTRICT FORM FOR CONSENT TO RELEASE CONFIDENTIAL STUDENT INFORMATION
A-2. STUDENT EDUCATIONAL RECORD ACCESS LOG
A-3. DATA USE AGREEMENT – SERVICES
A-4. DATA USE AGREEMENT – STUDIES
LAUSD HIPAA POLICY REGARDING STUDENT INFORMATION
LAUSD EMPLOYEE RECORD POLICY
DATA OWNER POLICY
LAUSD EMPLOYEE INFORMATION RESPONSIBILITY AGREEMENT

ASSISTANCE: For assistance or additional information, please call:
Carl Piper, Assistant General Counsel, (213) 241-7600

LAUSD FERPA POLICY
THE LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY ON PROTECTION OF STUDENT RECORDS

State and federal laws strictly regulate the protection of students' educational record information. This policy describes the protections required by law. Violations of this policy could result in a lawsuit against the District and/or any employee that permits an improper disclosure.

This "Family Educational Rights and Privacy Act (FERPA)" policy must be followed any time there is a request for access to, or the possibility of the "disclosure" of, the contents of a student's educational records. As used in this policy, "disclosure" means to permit access to or the release or other communication of information contained in student records, by any means, including oral, written, or electronic. Please note that improperly disposing of student records can constitute a "disclosure" under the law. Use secure disposal methods, such as the shredding of paper records.

In any case where there is a question about whether student record information should be disclosed, contact the Office of the General Counsel as soon as possible. In all cases, disclosure may occur only in accordance with the terms of this policy.

1. What kind of information is being requested?

Two general categories of student information must be protected by all District employees— "Confidential Student Information" and "Directory Information." The following general rules apply:

"Confidential Student Information"

"Confidential Student Information" includes any item of information, other than Directory Information, that is directly related to an identifiable District student and is maintained in the student's educational records or in any files maintained by a District employee. The format of the information does not matter—items recorded by handwriting, print, tapes, film, microfilm, on the hard disk, or any means, can all qualify as Confidential Student Information. The general rule is that Confidential Student Information may not be released without written consent from a parent or legal guardian. Exceptions to this rule are detailed below. In any event, Confidential Student Information may only be disclosed in accordance with this policy.

If you have any questions about whether or not Confidential Student Information may be disclosed, contact the Office of the General Counsel before any disclosure is made.

"Directory Information"

"Directory information" means a student's name, address, telephone number, date and place of birth, dates of attendance, and most recent previous public or private school attended. Student email addresses, and class schedules are not considered Directory Information and generally may not be released without consent.

Directory Information may not be disclosed to or accessed by private, profit-making entities other than the following: Parent Teacher Student Association; Elected Officials; Los Angeles County Departments of Health, Children and Family Services, Mental Health and Probation; United States Armed Forces (Military) Recruiting Agencies; Colleges, Universities or Other Institutions of Higher Education (including for-profit accredited institutions); the National Student Clearinghouse to track college attendance, Los Angeles County Departments Health Related Services (Department of Public Health and Department of Health Care Services), LAUSD School-based Health Care Providers, and the LA Trust for Children's Health.

A student's parent or legal guardian (or, in some cases, a student if over 18 years old) may notify the District of any information they refuse to permit the District to designate as directory information about that student. This designation will remain in effect until the parent or legal guardian (or, in some cases, the student) modifies this designation in writing. When this notification has been made, written consent is required before disclosing the applicable Directory Information relating to that student. The procedure for obtaining consent is described below. Questions about releasing Directory Information should be directed to the Office of the General Counsel.

2. Is there an emergency requiring the disclosure of student information?

Any time an emergency creates an immediate danger to the health or safety of a student or other individual, consent is not required to disclose Confidential Student Information to persons in a position to deal with the emergency, as long as (1) the emergency has been verified by a teacher or other school official, and (2) knowledge of the Confidential Student Information is necessary. Disclosure should be limited to only that Confidential Student Information that is necessary under the circumstances.

3. Who is requesting access to student records?

A request for disclosure of Confidential Student Information will come from one of these four kinds of requesters: (1) the student or his or her parent; (2) a District employee; (3) a representative or agent of a state or federal government other than a District employee, such as representatives of departments of education, law enforcement agencies, and state and federal courts; or, (4) a third party not within any of the first three categories. Each of these possible requesters is discussed below.

For purposes of this policy, a student's "parent" is his or her natural parent, adopted parent, or legal guardian. If a student's parents are divorced or legally separated, only the parents with

custody have rights under this policy unless the student's file contains a written agreement signed by both parents indicating that either parent may access student records and give consent to disclosure.

Requests from Parents and Students

Confidential Student Information may be disclosed to students and parents as follows:

The parent of a currently enrolled or former student who is under the age of 18 may access Confidential Student Information concerning his or her student, as may the parent of any student over the age of 18 who is considered a "dependent."

Any student who is 16 years of age or older, or who has completed the 10th grade, may access Confidential Student Information about himself or herself.

Once a student reaches the age of 18 and is not considered to be a dependent of the parent, the student is thereafter the only person who is entitled to exercise rights related to, and grant consent for the disclosure of, his or her Confidential Student Information contained in those records.

Requests from District Employees and Representatives

Confidential Student Information may only be disclosed to District staff who will be using the information for internal District purposes in connection with their assigned duties and have a legitimate interest in the information. District representatives include teachers, school administrators, and District administrative personnel. In addition, Confidential Student Information may be disclosed without consent to any established member of a school attendance review board who has a legitimate educational interest in the requested information. Disclosure to any other District employee or representative for any other purpose (including for any use by persons or organizations outside the District) requires written consent from the student's parent or legal guardian.

Requests from Government Representatives

Any request for Confidential Student Information from an agency, official, or other representative of a state or federal government must be promptly referred to the Office of the General Counsel, which will respond to the request. Examples of this kind of request include a subpoena, summons or other demand by a court or administrative tribunal, a request from a probation officer conducting any kind of investigation, or a request made by a police officer, state or federal criminal investigator, or a truancy officer. Requests from District Police do not require referral to the Office of General Counsel.

Requests from Third Parties

The general rule is that Confidential Student Information cannot be released to third parties without written consent from a parent or legal guardian. There are, however, exceptions. Confidential student information may be disclosed without consent in response to a request from:

- Officials at private schools and in other school systems where a student intends or seeks to enroll;
- Agencies or organizations requesting information in connection with a student's application for, or receipt of, financial aid (but only as may be necessary to determine the student's eligibility for financial aid, the amount of the financial aid, the conditions that will be imposed in connection with the financial aid, or to enforce the conditions of the financial aid); and
- County elections officials, only for the purpose of identifying students who are eligible to vote and conducting programs offering students the opportunity to register to vote.

Among third parties with whom the District will share Confidential Student Information without consent are vendors who are either performing services normally performed by District employees or are conducting studies to improve instruction. In these cases the District will enter into a Data Use Agreement with such vendors. Examples of such Data Use Agreements are provided in Attachments A-3 and A-4.

The District may provide aggregate and statistical data to third parties where such data is not personally identifiable to any individual student. Under FERPA, the definition of personally identifiable information includes "any set of facts that makes a student's identity easily discernable." Therefore, the demographic break down of the student population from which the data is extracted and the size of the pool of students used for such data analysis must be taken into consideration and care must be taken so that it is not easy to discern any individual student's identity. Further, no information that could be used to identify a student, such as student identification number, address, telephone number or social security number may be included.

For all other requests from third parties, consent must be obtained before Confidential Student Information may be disclosed. All questions about disclosing Confidential Student Information to a third party, or about the manner in which consent must be obtained, should be referred to the Office of General Counsel as quickly as possible after receipt of any request.

Requests from Military Recruiters

The No Child Left Behind Act requires secondary schools to provide students' names, addresses, and telephone listings to military recruiters and to institutions of higher education when they request that information. The District is required to provide this information unless the parent, guardian or, in some cases, the student, has made an election to refuse to allow disclosure of that information without prior written consent.

4. Has the proper written consent been obtained?

"Consent" under this policy means written consent, which must come either from a student's parent or an adult student, as applicable. Consent must be obtained on the District's standard form for consenting to the disclosure of Confidential Student Information, and all blanks on the form must be fully and accurately completed before

any information may be released. Any consent to disclose Confidential Student Information (which includes Directory Information for those students whose file includes a written request to withhold Directory Information) must specify the student records to be released, identify the party or class of parties to whom the records may be released, and be permanently kept within the student's cumulative file. A copy of the District's consent form is attached to this policy (Attachment A-1).

5. Has the disclosure been recorded in the student's access log?

Every student's file must contain a log or record (the "access log") that lists all persons, agencies, or organizations requesting or receiving information from the file and the reason(s) for the request. An access log may be inspected only by the student's parent (or the adult student, if applicable), the dependent adult student, and the student who is 16 years of age or older or who has completed the 10th grade. All other requests to inspect the access log must be referred to the Office of the General Counsel.

Access log entries must include:

- the name of the person(s) to whom information was disclosed (or, if no disclosure was made, from whom the request was received);
- the reason for disclosure;
- the time and circumstances of disclosure; and
- the particular records that were disclosed.

A sample access log is attached to this policy (Attachment A-2). The access log must identify each disclosure of Confidential Student Information, except that the access log need not list the following:

- Disclosures to parents, adult students, and students who have reached the age of 16 or have completed the 10th grade; Disclosures to District teachers requesting information about the students they are teaching;
- Disclosures to other District staff accessing information in connection with their assigned duties;
- Disclosures of Directory Information only; and
- Disclosures to anyone for whom written consent has been executed by the parent (or adult student, as applicable), as long as the written consent has been filed in the student's cumulative file.

6. Are there any other questions or concerns?

Any and all other questions and concerns about student record information and the disclosure of any student record information should be directed to the Office of the General Counsel, which can assist in all matters related to this policy and in complying with its terms.

DISTRICT FORM FOR CONSENT TO RELEASE CONFIDENTIAL STUDENT INFORMATION

[NOTE—REVIEW SCHOOL'S CURRENT CONSENT FORM FOR THE ELEMENTS BELOW]

STUDENT'S NAME: _____

STUDENT'S DATE OF BIRTH: _____ **NAME SCHOOL:** _____

CHECK ONE:

[ ] I am the _____ of the above named student, a non-emancipated
(Parent or Legal Guardian)
Student under the age of 18. I hereby consent to the release of confidential student information relating to this student.

[ ] I am an emancipated student or student over 18 years of age. I hereby consent to the release of my confidential student information.

CHECK ONLY IF APPLICABLE:

[ ] Purpose of Release—If consent is being given to release this information for a particular purpose, please describe this purpose: _____

[ ] Time Limit—If consent is being given to release this information during a particular period of time, please write the beginning date and ending date of consent:

_____ _____
Beginning Date Ending Date

[ ] I do **NOT** want my student's Directory Information (Name, Address, or Telephone Number) released to anyone, including the U.S. Military, other than as required by law.

SIGNED: _____ **DATE:** _____

STUDENT EDUCATIONAL RECORD ACCESS LOG

A student educational record access log must be kept in each District student's file, and must be completed every time there is a request for access to Confidential Student Information from a student's file. For more information on Confidential Student Information and when it may be disclosed, please refer to the Los Angeles Unified School District Policy on Protection of Student Records. Please contact the Office of the General Counsel with any questions regarding Confidential Student Information, this access log, or the aforementioned policy. The contents of this access log may not be disclosed except in accordance with the aforementioned policy.

Student Name: _____ **Name of School:** _____
Last Name **First Name** **Middle Name**

Date of Request for Disclosure	Name of Person(s) Requesting Disclosure	Disclosure Granted (Y/N)?	Reason for Disclosure	Date, Time and Circumstances of Disclosure	Particular Student Records Disclosed

DATA USE AGREEMENT

BETWEEN

THE LOS ANGELES UNIFIED SCHOOL DISTRICT

AND

CONTRACTOR NAME

FOR

THE DISCLOSURE OF EDUCATION RECORDS

1. PARTIES

1.1 The Los Angeles Unified School District ("District") is a public school district organized and existing under and pursuant to the constitution and laws of the State of California and with a primary business address at 333 S. Beaudry Avenue, Los Angeles, California 90017.

1.2 Contractor Name (Contractor) provides **CONTRACTOR TO INSERT DESCRIPTION** with a primary place of business at 123 Main Street, Any Town, USA 12345.

2. PURPOSE

2.1 The purpose of this Data Use Agreement ("Agreement") is to allow for the District to provide Contractor with personally identifiable information ("PII") from student education records ("student data") without consent so that the Contractor may perform the following institutional service or function for which the District would otherwise use employees:

CONTRACTOR TO INSERT DESCRIPTION

2.2 This Agreement is meant to insure that Contractor adheres to the requirements concerning the use of student information protected under the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. §1232g, 34 Code of Federal Regulations Part 99, and California Education Code sections 49060-49085. This agreement applies to all interactions between Contractor and District schools.

2.3 34 C.F.R. §99.30 and Education Code §49076(a) require the consent of the education rights holder prior to the release of PII from the education record of a student. An exception to the consent requirement is provided for in 34 CFR §99.31(a)(1)(i) and Education Code §49076(a)(2)(G)(i) for contractors "performing institutional services or functions otherwise performed by school employees." These contractors are considered "school officials" under FERPA and the California Education Code.

2.4 Under this Agreement, the District considers Contractor to be such a school official with legitimate educational interests performing an institutional service or function for which the District would otherwise use employees within the meaning of 34 C.F.R. §99.31(a)(1)(i) and Education Code

§49076(a)(2)(G)(i) and this allows the District to disclose PII from education records of students without the consent required by 34 C.F.R. § 99.30 and Education Code §49076(a).

2.6 This Agreement does not necessarily describe the complete nature of all interactions between the Contractor and the District. Rather, this Agreement pertains to the disclosure of personally identifiable information from education records only. It is likely that the Contractor has some other form of written agreement with the District (possibly including, but not limited to a separate contract or MOU, a license agreement, a subscription agreement, etc.). However, in so far as it pertains to the subject matter of this Agreement, this Agreement takes precedence over any inconsistencies with any other agreements.

3. PROCESS FOR DATA TRANSFER

The District entered into a five-year Contract August 1, 2015 with Clever, Inc., ("Clever") and EduTone Corporation (EduTone) under which Clever or EduTone receives electronic data from the District containing student, teacher, and other information. Clever or EduTone then provides the data to various District vendors, such as Contractor. This alleviates work on the District's part which formerly required the creating of separate record layouts for each vendor. By entering into this Agreement the District authorizes Clever or EduTone to send data to Contractor in accordance with the District's Contract with Clever.

4. DISTRICT DUTIES

4.1 The District will provide student data in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232g and 34 C.F.R. 99, and California Education Code sections 49060-49085.

The following student data will be provided:

CONTRACTOR TO INSERT DESCRIPTION

5. CONTRACTOR DUTIES

5.1 The Contractor will perform the following duties in regard to any student data it obtains:

5.1.1 Not disclose the information to any other party without the consent of the parent or eligible student;

5.1.2 Use the data for no purpose other than the work stated in this Agreement;

5.1.3 Allow the District access to any relevant records for purposes of completing authorized audits;

5.1.4 Require all employees, contractors and agents of any kind to comply with all applicable provisions of FERPA and other federal and California laws with respect to the data shared under this Agreement;

5.1.5 Designate in writing a single authorized representative able to request data under this Agreement. The authorized representative shall be responsible for transmitting all data requests and maintaining a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the completion of any projects and the return or destruction of data as required by this Agreement. District or its agents may, upon request, review the records required to be kept under this section;

5.1.6 Maintain all data obtained pursuant to this Agreement in a secure computer environment and not copy, reproduce or transmit data obtained pursuant to this Agreement except as necessary to fulfill the purpose of this Agreement. All copies of data of any type, including any modifications or additions to data from any source that contains information regarding students, are subject to the provisions of this Agreement in the same manner as the original data. The ability to access or maintain data under this Agreement shall not under any circumstances transfer from Contractor to any other institution or entity;

5.1.7 Destroy or return all personally identifiable information obtained under this Agreement when it is no longer needed for the purpose for which it was obtained no later than 60 days after it is no longer needed. In the event Contractor destroys the PII, Contractor shall provide the District with certification of such destruction. Failure to return or destroy the PII will preclude Contractor from accessing personally identifiable student information for at least five years as provided for in 34 C.F.R. section 99.31(a)(6)(iv).

5.2 If Contractor is an operator of an Internet website, online service, online application, or mobile application, Contractor shall comply with the requirements of California Business and Professions Code section 22584 and District policy as follows:

5.2.1 Contractor shall not (i) knowingly engage in targeted advertising on the Contractor's site, service or application to District students or their parents or legal guardians; (ii) use PII to amass a profile about a District student; (iii) sell information, including PII; or (iv) disclose PII without the District's written permission.

5.2.2 Contractor will store and process District Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Contractor warrants that all electronic District Data will be encrypted in transmission using SSL [(Secure Sockets Layer)] [or insert other encrypting mechanism] (including via web interface) [and stored at no less than 128-bit level encryption]. "Encryption" means a technology or methodology that utilizes an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, and such confidential process or key that might enable decryption has not been breached, and shall have the meaning given to such term under HIPAA and HIPAA Regulations, including 45 CFR §164.304.

5.2.3 Contractor shall delete a student's covered information upon request of the District.

5.2.4 District Data will not be stored outside the United States without prior written consent from the District.

5.3 Contractor shall comply with the District's information- security specifications prior to receiving any electronic transfers of pupil record information from any District-approved third party contractor, such as Clever or EduTone. District may require Contractor to provide documentation of compliance prior to any transmittal.

5.4 If Contractor will (1) provide cloud-based services which will involve digital storage of pupil records or (2) provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records, then, the following requirements in compliance with California Education Code section 49073.1 pertain:

5.4.1 The pupil records continue to be the property of and under the control of the District;

5.4.2 Contractor will not use any information in the pupil record for any purpose other than those required or specifically permitted by this Agreement.

5.4.3 In order for a parent, legal guardian or eligible pupil to review personally identifiable information in the pupil's records and correct erroneous information, Contractor shall:

CONTRACTOR TO INSERT DESCRIPTION

5.4.4 Contractor shall take the following actions, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records:

CONTRACTOR TO INSERT DESCRIPTION

5.4.5 Contractor shall use the following procedure for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records:

CONTRACTOR TO INSERT DESCRIPTION

5.4.6 Contractor certifies that it will not retain the pupil records upon completion of the services. Contractor will take the following actions to enforce this certification:

CONTRACTOR TO INSERT DESCRIPTION

5.4.7 Contractor shall not use personally identifiable information in pupil records to engage in targeted advertising.

5.4.8 The following shall be considered a part of and required under this Agreement:

- **The District's Contractor Code of Conduct** (http://achieve.lausd.net/cms/lib08/CA01000043/Centricity/Domain/218/5.%20%20CODE%20OF%20CONDUCT%20irfp.pdf)
- **SB 1177 Student Online Personal Information Protection Act (SOPIPA)**

(Effective 1/1/16)
(https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177)

5.5 **Additional Contractor Duties Pertaining to Protected Information**

5.5.1 In addition to any Contractor obligations stated elsewhere in this Agreement, Contractor shall notify the District in writing as soon as possible, but in no event more than two (2) business days, after Contractor becomes aware of any breach security or any security incident involving the District's **PROTECTED INFORMATION** (see Section 2.2). Contractor shall be deemed to be aware of any breach or security incident as of the first day on which such breach or security incident is known or reasonably should have been known to its officers, employees, agents, or subcontractors. Contractor shall identify as soon as practicable each individual whose unsecured **PROTECTED INFORMATION** has been, or is reasonably believed by Contractor to have been, accessed, acquired, or disclosed during such breach or security incident. Contractor shall cooperate in good faith with the District in the investigation of any breach or security incident.

5.5.2 Contractor shall take prompt corrective action to remedy any breach or security incident, mitigate, to the extent practicable, any harmful effect of a use or disclosure of **PROTECTED INFORMATION**, and take any other action required by applicable federal and state laws and regulations pertaining to such breach or security incident.

5.5.3 Contractor will provide written notice to the District as soon as possible but no later than twenty (20) calendar days after discovery of the breach or security incident of the actions taken by Contractor to mitigate any harmful effect of such breach or security incident and the corrective action Contractor has taken or shall take to prevent future similar breaches or security incidents. Upon the District's request, Contractor will also provide to the District a copy of Contractor’s policies and procedures that pertain to the breach or security incident involving the District's **PROTECTED INFORMATION**, including procedures for curing any material breach of this Agreement.

5.5.4 Contractor shall make reasonable efforts to trace lost or translate indecipherable transmissions. Contractor shall bear all costs associated with the recreation of incomplete, lost or indecipherable transmissions if such loss is the result of an act or omission of Contractor.

5.5.5 Contractor shall take appropriate security measures to protect the confidentiality, Integrity, and availability of the District's **PROTECTED INFORMATION** that it creates receives, maintains, or transmits on behalf of the District and to prevent any use or disclosure of the District's **INFORMATION** other than as provided by the Agreement. Appropriate security measures include the implementation of the best practices as specified by the ISO 27001/2, NIST, or similar security industry guidelines.

6. AUTHORIZATION FOR TRANSFER OF DATA.

6.1 The District hereby authorizes Contractor to receive the student data listed in Section 4.2.

6.2 Contractor agrees that District makes no warranty concerning the accuracy of the student data provided.

7. TERM

7.1 This Agreement shall be effective on the date the last party signs and shall be for an indefinite term to match any Contractor interactions with the District under which the Contractor receives student data.

7.2 Either party may terminate this Agreement for any reason at any time upon reasonable notice to the other party.

8. NOTICES

8.1 All notices required or permitted by this Agreement shall be in writing and shall be either personally delivered or sent by nationally-recognized overnight courier, facsimile, email or by registered or certified U.S. mail, postage prepaid, addressed as set forth below (except that a party may from time to time give notice changing the address for this purpose). A notice shall be effective on the date personally delivered, on the date delivered by a nationally-recognized overnight courier, on the date set forth on the email or on the receipt of a telecopy or facsimile, or upon the earlier of the date set forth on the receipt of registered or certified mail or on the fifth day after mailing.

8.2 Notices shall be delivered to the following:

DISTRICT:

Attention: Oscar Lafarga
Office of Data and Accountability
333 South Beaudry Avenue, 16th Floor
Los Angeles, CA 90017

CONTRACTOR:

Attention:
Contractor Name
123 Main Street
Any Town, USA 12345

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

LOS ANGELES UNIFIED SCHOOL DISTRICT

By: _____ Date: _____

Title/Position: _____

Contractor

By: _____ Date: _____

Title/Position: _____

DATA USE AGREEMENT

BETWEEN

THE LOS ANGELES UNIFIED SCHOOL DISTRICT

AND

PARTY

FOR

DATA SHARING [STUDIES/ RESEARCH]

PARTIES

1. The Los Angeles Unified School District (the District) is a public school district organized and existing under and pursuant to the constitution and laws of the State of California and with a primary business address at 333 S. Beaudry Avenue, Los Angeles, California 90017.

2. (Contractor) is located at_____.

PURPOSE

3.1 The purpose of this Data Use Agreement ("Agreement) is to provide the District with_____. This Agreement is meant to ensure that Contractor adheres to the District's requirements concerning use of student information and applies to studies/ research conducted by District schools.

3.2 The disclosure of personally identifiable information from student education records is for, or on behalf of the District, in order to improve instruction.

3.3 Explain the purpose/ legitimate interest for the studies.

3.4 The District entered into a five-year Contract August 1, 2015 with Clever, Inc., ("Clever") and EduTone Corporation (EduTone) under which Clever or EduTone receives electronic data from the District containing student, teacher, and other information. Clever or EduTone then provides the data to various District vendors, such as Contractor. This alleviates work on the District's part which formerly required the creating of separate record layouts for each vendor. By entering into this Agreement the District authorizes Clever or EduTone to send data to Contractor in accordance with the District's Contract with Clever.

DUTIES

4. The District will perform the following duties:

4.1 Provide data through Clever in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232g and 34 C.F.R. 99, and California Education Code sections 49060-49085.

5. The Contractor will perform the following duties:

5.1 Comply with all FERPA and California Education Code provisions, including the following:

5.1.1 Use the data shared under this Agreement for no purpose other than the work stated in this Agreement and in Contractor's agreements with District schools and authorized under Section 99.31(a)(6) of Title 34 of the Code of Federal Regulations. Contractor further agrees not to share data received under this Agreement with any other entity. Contractor agrees to allow LAUSD access to any relevant Contractor records for purposes of completing authorized audits.

5.1.2 Require all employees, contractors and agents of any kind to comply with all applicable provisions of FERPA and other federal and California laws with respect to the data shared under this Agreement.

5.1.3 Maintain all data obtained pursuant to this Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to this Agreement except as necessary to fulfill the purpose of the original request. All copies of data of any type, including any modifications or additions to data from any source that contains information regarding students, are subject to the provisions of this Agreement in the same manner as the original data. The ability to access or maintain data under this Agreement shall not under any circumstances transfer from Contractor to any other institution or entity.

5.1.4 Not disclose any data obtained under this Agreement in a manner that could identify an individual parents and students to any other entity in published results of studies as authorized by this Agreement.

5.1.5 Destroy all personally identifiable data obtained under this Agreement when it is no longer needed for the purpose for which it was obtained. Nothing in this Agreement authorizes Contractor to maintain personally identifiable data beyond the time period reasonably needed to complete the purpose of the request. All personally identifiable data shall be destroyed in compliance with 34 CFR Section 99.31(a)(6). Contractor agrees to require all employees, contractors, or agents of any kind to comply with this provision.

5.2

If Contractor is an operator of an Internet website, online service, online application, or mobile application, Contractor shall comply with the requirements of California Business and Professions Code section 22584 and District policy as follows:

5.2.1 Contractor shall not (i) knowingly engage in targeted advertising on the Contractor's site, service, or application to District students or their parents or legal guardians; (ii) use PII to amass a profile about a District student; (iii) sell information, including PII; or (iv) disclose PII without the District's written permission.

5.2.2 Contractor will store and process District Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Contractor warrants that all electronic District Data will be encrypted in transmission using SSL [(Secure Sockets Layer)] [or insert other encrypting mechanism] (including via web interface) [and stored at no less than 128-bit level encryption].

5.2.3 Contractor shall delete a student's covered information upon request of the District.

5.2.4 District Data will not be stored outside the United States without prior written consent from the District.

5.3 Contractor shall comply with the District's information security specifications prior to receiving any electronic transfers of pupil record information from Clever. District may require Contractor to provide documentation of compliance prior to any transmittal.

5.4 If the Contractor will provide cloud-based services which will involve digital storage, management and retrieval of pupil records or will provide digital educational software to access, store, and use pupil records, the following requirements in compliance with California Education Code section 49073.1 pertain:

5.4.1 The pupil records continue to be the property of and under the control of the District;

5.4.2 Contractor will not use any information in the pupil record for any purpose other than those required or specifically permitted by this Agreement.

5.4.3 In order for a parent, legal guardian or eligible pupil to review personally identifiable information in the pupil's records and correct erroneous information, Contractor shall:

CONTRACTOR TO DESCRIBE

5.4.4 Contractor shall take the following actions, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records:

CONTRACTOR TO DESCRIBE

5.4.5 Contractor shall use the following procedure for notifying the affected

parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records:

CONTRACTOR TO DESCRIBE

5.4.6 Contractor certifies that it will not retain the pupil records upon completion of the services. Contractor will take the following actions to enforce this certification:

CONTRACTOR TO DESCRIBE

5.4.7 Contractor shall not use personally identifiable information in pupil records to engage in targeted advertising.

5.5 Pre-Publication Review. Upon notice, District may request and Contractor agrees to timely provide, prior to publication or re-publication, access to any report, memorandum, article, thesis or any other writing that includes Student Record Information provided under this Agreement and links District to any outcome or enables District to be linked to any outcome. District reserves the right to withdraw consent to the publication of any such writing if the District determines that the privacy rights of its students or interests of the District are jeopardized, or such writing contains statements or facts that the District considers untrue or unacceptable for publication.

AUTHORIZATION FOR TRANSFER OF DATA

6. The District hereby authorizes Contractor to receive data from Clever or EduTone and Clever or EduTone to send such data to Contractor.

DATA AUTHORIZED FOR TRANSFER

7.1 The data listed in Contractor's "Data Collection FAQ" (Attachment 2) and "IL Import Template" (Attachment 3) is authorized for transfer.

7.2 Contractor agrees that District makes no warranty concerning the accuracy of the student data provided.

TERM

8. This Agreement shall be effective for five year/s (maximum of five years) from the date the last party signs. Either party may terminate this Agreement for any reason at any time upon reasonable notice to the other party.

GENERAL PROVISIONS

9. INDEPENDENT CONTRACTOR While engaged in performance of this Agreement the Contractor is an independent contractor and is not an officer, agent, or employee of the

District. Contractor is not entitled to benefits of any kind to which District's employees are entitled, including but not limited to unemployment compensation, workers' compensation, health insurance, and retirement benefits. Contractor assumes full responsibility for the acts and/or omissions of Contractor's employees or agents as they relate to performance of this Agreement. Contractor assumes full responsibility for workers' compensation insurance, and payment of all federal, state and local taxes or contributions, including but not limited to unemployment insurance, social security, Medicare, and income taxes with respect to Contractor and Contractor's employees. Contractor warrants its compliance with the criteria established by the U.S. Internal Revenue Service (I.R.S.) for qualification as an independent contractor, including but not limited to being hired on a temporary basis, having some discretion in scheduling time to complete contract work, working for more than one employer at a time, and acquiring and maintaining its own office space and equipment. Contractor agrees to indemnify District for all costs and any penalties arising from audits by state and/or federal tax entities related to services provided by Contractor's employees and agents under this Agreement.

10. CONFLICT OF INTEREST Contractor represents that Contractor has no existing financial interest and will not acquire any such interest, direct or indirect, which could conflict in any manner or degree with the performance of services required under this Agreement and that no person having any such interest shall be subcontracted in connection with this Agreement, or employed by Contractor. Contractor shall not conduct or solicit any non-District business while on District property or time.

10.1 Contractor will also take all necessary steps to avoid the appearance of a conflict of interest and shall have a duty to disclose to the District prior to entering into this Agreement any and all circumstances existing at such time which pose a potential conflict of interest.

10.2 Contractor warrants that it has not directly or indirectly offered or given, and will not directly or indirectly offer or give, to any employee, agent, or representative of District any cash or noncash gratuity or payment with view toward securing any business from District or influencing such person with respect to the conditions, or performance of any contracts with or orders from District, including without limitation this Agreement. Any breach of this warranty shall be a material breach of each and every contract between District and Contractor.

10.3 As a condition of this Agreement, Contractor agrees to comply with the "Contractor's And Consultant's Code Of Conduct" set forth in the Los Angeles Unified School District Contractor's And Consultant's Code Of Conduct which is attached hereto as Attachment D and made a part hereof.

10.4 Should a conflict of interest issue arise, Contractor agrees to fully cooperate in any inquiry and to provide the District with all documents or other information reasonably necessary to enable the District to determine whether or not a conflict of interest existed or exists.

10.5 Failure to comply with the provisions of this section shall constitute grounds for immediate termination of this Agreement, in addition to whatever other remedies the District may have.

11. EQUAL EMPLOYMENT OPPORTUNITY It is the policy of the District that, in connection with all work performed under District agreements, there shall be no discrimination against any employee or applicant for employment because of race, color, religious creed, national origin, ancestry, marital status, sex, sexual orientation, age disability or medical condition and therefore and therefore the contractor agrees to comply with applicable federal and state laws. In addition, the Contractor agrees to require like compliance by all subcontractors employed on the work.

12. GOVERNING LAW The validity, interpretation and performance of this Agreement shall be determined according to the laws of the State of California.

13. INDEMNIFICATION Contractor shall indemnify and hold the District and its Board Members, administrators, employees, agents, attorneys, and contractors ("Indemnitees") harmless against all liability, loss, damage and expense (including reasonable attorneys' fees) resulting from or arising out of this Agreement or its performance, whether such loss, expense, damage or liability was proximately caused in whole or in part by the negligent or willful act or omission of Contractor, including, without limitation, its agents, employees, subcontractors or anyone employed directly or indirectly by it.

14. INSURANCE Contractor shall, at his, her, or its sole cost and expense, maintain in full force and effect, during the term of this Agreement, the following insurance coverage from a California licensed and/or admitted insurer with an A minus (A-), VII, or better rating from A.M. Best:

A. Commercial General Liability Insurance with limits as follows:
- $1,000,000 per occurrence
- $1,000,000 personal & advertising injury
- $2,000,000 general aggregate
- $1,000,000 products/completed operations aggregate

B. The Commercial General Liability policy must contain coverage for personal and advertising injury to protect against any claim of:

- Libel
- Slander
- Copyright or trademark infringement
- Invasion of privacy

The commercial general Liability policy must provide a defense and indemnity for the above type of claims, and such claims as those in Paragraph B of this section must not be excluded under the personal and advertising injury coverage of the policy.

C. Any deductibles or Self-Insured Retentions (SIR) shall be declared in writing, and all deductibles and retentions above $25,000 require District

approval

D. Contractor, upon execution of this contract and periodically thereafter upon request, shall furnish the District with certificates of insurance evidencing such coverage. The certificate of insurance shall include a thirty (30) day non-renewal/cancellation notice provision. The Commercial General Liability policy referred to in Paragraph A of this section shall name the District and the Board of Education as additional insured.

15. NOTICES All notices required or permitted by this Agreement shall be in writing and shall be either personally delivered or sent by nationally-recognized overnight courier, email, facsimile or by registered or certified U.S. mail, postage prepaid, addressed as set forth below (except that a party may from time to time give notice changing the address for this purpose). A notice shall be effective on the date personally delivered, on the date delivered by a nationally-recognized overnight courier, on the date set forth on the e-mail or on the receipt of a telecopy or facsimile, or upon the earlier of the date set forth on the receipt of registered or certified mail or on the fifth day after mailing.

DISTRICT:	CONTRACTOR:
Attention: Oscar Lafarga	Attention:
Office of Data and Accountability	_____
333 South Beaudry	_____
Avenue, 16th Floor Los	_____
Angeles, CA 90017	
TEL:	TEL:
FAX:	FAX:

IN WITNESS WHEREOF, the parties have executed this Agreement as of the last day noted below. LOS ANGELES UNIFIED SCHOOL DISTRICT

By: _____ Date: _____
Title/Position: _____

CONTRACTOR

By: _____ Date: _____
Title/Position: _____

THE LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY ON THE PROTECTION OF HEALTH INFORMATION UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 REGARDING STUDENT INFORMATION

State and federal laws strictly regulate the protection of an individual's health information. Violating these laws could subject a District employee to disciplinary action, up to and including dismissal, as well as result in a lawsuit against the District and/or the employee who is in violation.

This policy is intended to help District employees follow those laws whenever they receive access or use a student's health-related information, or receive a request for access to that information. A separate attachment will be prepared regarding other types of health-related information. If you have any questions after reading this policy about whether a student's health information may be used or disclosed, you should contact the Office of the General Counsel immediately. Please note that improperly disposing of Personnel Records or Employee Information can constitute a "disclosure" under the law. Use secure disposal methods, such as the shredding of paper records.

1. What is HIPAA?

The Federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), established, for the first time, a set of national standards for the protection of an individual's health information. The federal government then published a set of regulations known as the HIPAA Privacy Rule that set forth how an individual's protected health information could be used and disclosed, and the ways in which individuals could control access to their health information.

Please note that the HIPAA Privacy Rule does <u>not</u> apply to information contained in an employee's employment record. That information is protected under other federal and state laws.

2. Why does HIPAA apply to the District?

The District, through certain of its divisions, affiliates, employees, and independent contractors, receives and retains records of health care services provided to students. The District also provides medical services to students. Under certain circumstances, a student's health information becomes part of the student's file. Thus, the District and its employees have access to student health information that is protected under HIPAA. Therefore, the District and its employees must comply with all relevant provisions of the HIPAA Privacy Rule.

3. What is a student's protected health information?

A student's protected health information ("PHI") is any information that both (a) identifies the student, including demographic information such as name, address, age, sex, social security number and date of birth, and (b) relates to the student's past, present or future physical or mental health or condition, or to the student's receipt of, or payment for, medical treatment or health care services. PHI does not include non-health care information contained in a student's educational records. Information contained in a student's educational records is protected under other federal and state laws, and that information is separately covered under the District's Policy on Protection of Student Records ("FERPA Policy," Attachment A).

4. How must protected health information be kept confidential?

Protected health information must be kept confidential at all times and may only be used and disclosed in accordance with this policy. This means you cannot disclose PHI to any other person unless authorized by this policy. This includes disclosures made verbally in person or by telephone, and in writing by mail, fax or e-mail. This prohibition on uses and disclosures also means that you cannot repeat information you hear, make copies of information you receive, or share passwords or login information with others unless authorized by this policy. There are serious legal penalties for the unauthorized use or disclosure of PHI. **Do not take any chances. Contact the Office of the General Counsel whenever you have a question about this policy or the use or disclosure of protected health information.** Please note improperly disposing of Personnel Records or Employee Information can constitute a "disclosure" under the law. Use secure disposal methods, such as the shredding of paper records.

5. When may protected health information be disclosed?

A student's protected health information may be disclosed directly to the student upon request by the student if the student is at least 18 years old, the student is an emancipated minor, or the student is requesting protected health information from a medical treatment for which the student is legally allowed to consent. If the student is under 18 years old, not emancipated or not legally allowed to consent to the medical treatment addressed in the protected health information, the student's PHI may be disclosed directly to the student's parent or legal guardian upon request from the parent or legal guardian, unless one of the following circumstances exists: (1) there is any suspicion or belief that the student has been or may be subjected to domestic violence, abuse, or neglect by the parent or legal guardian, (2) disclosing the student's PHI to the parent or legal guardian could endanger the student, or (3) the request relates to protected health information from a medical treatment that the student sought or obtained on a confidential basis. **If you are not sure whether to disclose a student's protected health information, please contact the Office of the General Counsel.**

A student's protected health information may be disclosed any time there is a serious and imminent threat to the health or safety of a student or other individual as long as (a) the threat has been verified by a health care professional, and (b) disclosure of the PHI is made to someone who can prevent or lessen the threat. PHI may also be used or disclosed by the District in connection with any internal activities of the District related to providing, payment for, or managing health care treatment and services. PHI may also be disclosed to health care providers for purposes of treating a student. In any case where you have a request for disclosure of protected health information that involves notes from psychotherapy or any similar treatment, promptly contact the Office of the General Counsel to discuss the request.

Any request from a government agency or official, a court of law, or any other representative of a state or federal government for a student's protected health information must promptly be referred to the Office of the General Counsel for response. In addition, if you believe that a use or disclosure of protected health information is required by law, such as in the case of possible incidents of child abuse, you must promptly refer the matter to the Office of the General Counsel.

Except as stated in this Section #5, a student's protected health information cannot be used or disclosed without the written authorization of the student, parent or legal guardian, as applicable.

6. Can I conduct a survey in which health related information is solicited from survey participants?

If you are gathering information but not gathering any identifiable information about the individual (such as their name or address) and there is no way to re-identify the individual once the survey has been submitted, then consent is not required. In the text of the survey, you must indicate that the information submitted is not protected by state or federal privacy rules. However, if you are gathering any identifiable information, consent from the subject, or his or her parent or guardian, is required along with certain notices, such as notice of what will be done with the information and how it will be stored.

For example, a survey on kids' exposure to violence that does not also solicit health related information, such as any mental or physical effect of such violence, is permissible. On the other hand, if the survey includes health information or information that could lead to a physical or mental health diagnosis, such as whether the child had problems sleeping or evidence of depression, the information must be kept confidential and consent of the parent, guardian or, in some cases, the student, is required in order to disclose the data. Similarly, basic physical data such as height, weight, and results of PE tests must be kept confidential and not disclosed without the consent of the parent, guardian or in some cases, the student. An exception to this rule is that such data may be disclosed if it is directory information of members of school sports teams and no restriction on disclosure has been submitted by the

parent, guardian or, in some cases, the student. On the other hand, data in aggregate form held in a manner that does not permit re-identification of a particular student may be disclosed, such as an announcement that a certain percentage of the student body at a high school passed a certain PE test.

7. How do I obtain a written authorization to disclose protected health information?

Except for disclosures set forth in Section #5 above, you must obtain a written authorization from the student, parent, or legal guardian prior to disclosing the student's protected health information to another person or organization. For example, if you receive a request from another school district or from a college or technical school for a student's records that contain protected health information, you must get a written authorization from the student, or from the student's parent or legal guardian if the student is under 18 years old, not emancipated or not legally permitted to consent to medical treatment, before you release any protected health information. [If the request is from a federal or state agency or court of law you must send the request to the Office of the General Counsel immediately.]

In order to obtain a written authorization, have the student, parent or legal guardian, as appropriate, complete and sign the District's form "Authorization to Release Protected Health Information." A copy of the form is attached to this policy. **The District's authorization form must be completed** regardless of whether you receive another authorization form with the request for the student's protected health information. The District's authorization form must be completely filled in and signed. Unless the disclosure is expressly permitted by Section #5, you cannot release any protected health information until you have the District's authorization form fully completed and signed by the student, the parent or the legal guardian (as appropriate).

Once the District's authorization form is completed and signed, you can only release the information stated in the form to be disclosed, and in no event can you disclose more information than was requested. For example, if the student's file contains protected health information for school years 1999-2002 and you receive a request for a student's health information for school years 1999-2002, but the authorization is only to release information for school year 2001-2002, you may only release the information for school year 2001-2002. On the other hand, if you receive a request for a student's health information for school years 2001-2002, but the authorization is to release all health information, you may still only release the health information for school years 2001-2002.

8. What other steps must be taken when protected health information is disclosed?

You must keep a record of each time you use or disclose a student's protected health information. Therefore, each time you receive a request for PHI, put a copy of the request in the student's file. If the request must be sent to the Office of the General Counsel for

response (See #5 above), make a copy of the request and place the copy in the student's file prior to sending the request to the Office of the General Counsel. If you obtain a written authorization to release the information, put a copy of the written authorization with the original request. You do not need to keep track of disclosures of a student's protected information if you give the PHI directly to the student, or the student's parent or legal guardian.

9. Where can I go for further information?

You should call the Office of the General Counsel at (213) 241-7600 if you have any questions or concerns about how to handle a student's protected health information. In addition, if you have any information about possible violations to this policy or the unauthorized use or disclosure of a student's protected health information, you should contact the Office of the General Counsel. You will not be penalized in any way for reporting such information.

Please be aware that the District is adopting this policy to comply with state and federal law, and is making it available for informational purposes only. This policy is not intended to provide you, or anyone else, with any rights, remedies, claims or causes of action whatsoever.

DISTRICT CONSENT FORM

AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION

(PLEASE PRINT)

DATE _____

STUDENT'S NAME: _____

STUDENT'S DATE OF BIRTH:_____**NAME OF SCHOOL:** _____

MY RELATIONSHIP TO THE STUDENT (FATHER, MOTHERGUARDIAN):

I HEREBY CERTIFY THAT I AM THE ABOVE STUDENT'S PARENT O R LEGAL GUARDIAN.

I HEREBY <u>CONSENT</u> TO THE DISCLOSURE BY THE LOS ANGELES UNIFIED SCHOOL DISTRICT OF THE ABOVE-REFERENCED STUDENT'S HEALTH RECORDS.

THIS CONSENT IS VALID UPON EXECUTION FOR A PERIOD OF 12 MONTHS AND MAY BE WITHDRAWN BY ME PRIOR TO THAT DATE ONLY BY WRITTEN NOTIFICATION.

_____ _____

PARENT OR GUARDIAN'S SIGNATURE **DATE**

_____

PRINT NAME

……

I HEREBY <u>WITHDRAW</u> CONSENT TO RELEASE THE ABOVE-REFERENCED STUDENT'S HEALTH RECORDS.

_____ _____

PARENT OR GUARDIAN'S SIGNATURE **DATE**

LAUSD EMPLOYEE RECORD POLICY

THE LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY ON PROTECTION OF EMPLOYEE RECORDS

From time to time, the District and its employees receive requests for access to private information about an employee. This private information consists of both Personnel Records and Employee Information.

This policy must be followed any time there is a request for access to, or the possibility of the "disclosure" of the contents of an employee's Personnel records or Employee Information. As used in this policy, "disclosure" means, "to permit access to or the release or other communication of information contained in employee records, by any means, including oral, written, or electronic." Please note that improperly disposing of Personnel Records or Employee Information can constitute a "disclosure" under the law. Use secure disposal methods, such as the shredding of paper records.

In any case where there is a question about whether employee Personnel Records or Employee Information should be disclosed, contact the Office of the General Counsel as soon as possible. In all cases, disclosure may occur only in accordance with the terms of this policy. Failure to follow these policies may result in discipline, including termination.

Some Personnel Records must be kept by the District indefinitely unless microfilmed or otherwise stored. For more information about these, check with Personnel.

The laws relating to the privacy of employee information come from many sources, including state and federal statutes. In ordinary situations, the State law applies to situations dealing with the privacy of the District's employee records. This is different from agency to agency, depending on the level of Federal control over the agency's day-to-day activities. Because the federal government does not exercise a great deal of control over the day-to-day operations of the District, state law applies, even though the District receives federal funding. If you have any questions about which laws apply, please direct them to the Office of the General Counsel.

1. **Are Personnel Records private?**

   Personnel Records are records kept by the District that may affect or be used relative to that employee's qualifications for employment, promotion, transfer, compensation, attendance or disciplinary action. It is the policy of the District to maintain the privacy of Personnel Records. District employees are permitted to view their own records under certain circumstances, as outlined below. Other District employees are permitted access to these records only where necessary to perform their job. Vendors are permitted access to these records when the information is required to provide services to the employee or District. When protected Employee Information must be transmitted to a vendor providing services to the employee or

District, the District shall require that the transmission be by the most secure method practical under the circumstances, and that the vendor keep the information strictly confidential.

2. Is Employee Information private?

Employee Information is information retained by the District about an employee that is not contained in an employee folder. Employee Information includes lists, reports or data on computer systems that are used by other departments or vendors to provide employees services such as payroll, healthcare and Workers' Compensation. Some types of Employee Information are protected, other types are not. Employee Information such as an employee's name, position, work phone number or workplace location is a matter of public record and not protected by law.

However, Employee Information is protected by this policy when, if released, it could result in an unwarranted invasion of an employee's personal privacy. Information of this sort is of a personal nature, with no relation to an employee's work duties or functions. Examples of this kind of "protected Employee Information" include an employee's home address, phone number, social security number, marital status, parental status, salary information, disciplinary information and other types of information of this nature. Although these are not "personnel records," it is the policy of LAUSD to maintain the privacy of this type of employee information except when this information must be accessed by employees of the District in order to perform their job functions, or by vendors requiring the information to provide services to the employee or the District. When this protected Employee Information must be transmitted to a vendor providing services to the employee or District, the District shall require that the transmission be by the most secure method practical under the circumstances as determined by the District Information Security Coordinator, and that the vendor keep the information strictly confidential. **If you are unsure as to whether this information is protected, contact the Office of the General Counsel prior to providing this information to anyone outside the District.**

3. Are there any other circumstances where Personnel Records or Employee Information may be released without employee consent?

Under some circumstances required by law, Personnel Records and/or Employee Information, even protected employee information, must be disclosed. An example would be where the names, telephone numbers, and last known addresses are requested in a subpoena arising out of a lawsuit with the District or a third party. All requests for Personnel Records or Employee Information from any internal or external party who does not require that information as part of their normal job function must be forwarded immediately to the Office of the General Counsel. In certain circumstances, such as when subpoenaed, information may be released unless the employee takes action in court or otherwise to prevent it from being released.

4. What kinds of Personnel Records does the District keep?

The District keeps several types of Personnel Records across multiple organizations within the District. There are five basic categories of personnel information: Service Information, Salary Allocation Information, Employee Relations Information, Health Information, and Supervisor's

Information. Below are the types of records contained in each category. Most of these records are accessible to employees on an appointment basis by the office that keeps the folder. The records that are not accessible are marked with an asterisk (*). These records can be described, to the extent possible, to the employee upon request.

A. Service Information (Employee Relations Department)

1. Applications for employment or reinstatement
2. Certification of citizenship and age
3. Requests for change in classification
4. Correspondence, including letters of reprimand
5. Credential material
6. Derogatory correspondence
7. Grievance Reports (final report)
8. Health approval forms
9. Leaves of Absence
10. Notices of unsatisfactory services or act
11. Oaths of allegiance
12. Performance evaluations, reports or commendations
13. References from inside District for initial employment
14. Report of notice of inadequate or unsatisfactory service
15. Resignations
16. Salary statements
17. Transcripts
18. Information from the Department of Motor Vehicles
19. Department of Justice, Criminal Background Check
20. Workers' Compensation Files
21. Attendance Records
22. Garnishments
23. * Placement files, university or college
24. * References from inside the District for initial employment (prior to 1965)
25. * References from inside the District for promotional exams
26. * References from outside the District

B. Salary Allocation Information (Salary Allocation Unit)

1. Application for Experience Credit
2. Application for Salary Point Credit
3. District in-service class forms
4. Official transcripts used for salary
5. Record of point credit for university and non-accredited institution work
6. Routine correspondence
7. Supplemental claims
8. Verification of previous experience

C. Employee Relations Information (Employee Relations Department)
Materials are released only to the Superintendent or his/her designated representative; they are not released to the examination committees, school principals, or supervisors.

1. Court records, conviction statements and related correspondence
2. Derogatory correspondence from inside and outside the District (subject to Education Code 44301)
3. Complaints and files under Board Rule 133
4. Medical appeal correspondence
5. Correspondence, including letters of reprimand
6. Subpoenas
7. * Arrest statements, police reports and fingerprints reports

D. Health Information (Coordinator, Employee Health)
1. Correspondence
2. Medical health record
3. Medical reports
4. Dependents' Information

E. Supervisor's Information (Your Supervisor)
1. Evaluations and Performance Expectations
2. Records relating to performance expectations
3. Derogatory correspondence from inside and outside the District (subject to Education Code 44031)

5. What do I do if I believe employee private personnel records and/or employee information have been released?

Tell your supervisor immediately. If you are a supervisor immediately notify the Office of the General Counsel if you believe any records relating to employees have been released inadvertently. There are strict laws relating to notice that must be followed, and failure to properly notify the proper party may result in disciplinary action, including but not limited to termination.

6. When should I contact the Office of the General Counsel?

As stated above, you should contact the Office of the General Counsel if you believe there has been a release of protected employee information, if there is a subpoena or Public Records Act request, if you receive unsubstantiated negative or inflammatory anonymous information about an employee, or if copies of, or access to, records are requested by a law enforcement agency.

DISTRICT FORM FOR CONSENT TO RELEASE

OF CONFIDENTIAL EMPLOYEE INFORMATION

EMPLOYEE NAME: _____ EMPLOYEE# _____

DIVISION: _____

SUPERVISOR: _____

I HEREBY CONSENT TO RELEASE EMPLOYEE CONFIDENTIAL EMPLOYEE INFORMATION TO THE FOLLOWING PARTIES:

_____

_____

OTHER CONDITIONS OF EMPLOYEE CONSENT TO RELEASE:

_____

_____

_____

PLEASE SIGN AND DATE (INVALID WITHOUT SIGNATURE):

SIGNED: _____ DATE: _____

PLEASE PRINT NAME: _____

DATA OWNER POLICY

THE LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY ON DATA OWNERSHIP ASSIGNMENT AND RESPONSIBILITY

District Bulletin No. 1077.2, Information Protection Policy, establishes that designated individuals will have management responsibility for District information, whether the information is electronically processed or available only on paper. The designated individual, known as the Data Owner, will have the final decision-making authority over information release and subsequent information use.

This policy is intended to help District employees follow this policy by providing a guide to District applications and their assigned Data Owners. Where District staff has questions regarding information disclosure, security, or proper handling, the assigned Data Owner is the primary contact. Where the Data Owner is ambiguous, unknown, or not specified, additional policies and procedures are provided to ensure the District's information protection policies are followed.

1. When does this policy apply?

This policy must be consulted whenever a request is received to disclose or provide District information in any form. The request may originate with a District employee, a District vendor, a student, a student's parents or guardians, or any other party. This policy establishes procedures that must be followed before releasing District information to any individual who is not routinely granted access as part of their normal job duties.

This policy should also be consulted whenever decisions are to be made regarding information protection. Information protection includes protection of hardcopy printed material, computers, communications facilities, and computer storage media (flash drive, magnetic tape, CD-ROM, etc.). Information designated “Protected” has special legal requirements for protection that must be followed.

2. What if no Data Owner is listed for the specific system?

At times a Data Owner may be assigned to an entire group of similar systems, without each member of the group being explicitly listed. Systems may also go by different names than those listed. The absence of a system from this list does not always mean the Data Owner is unassigned.

The Office of the General Counsel should be contacted to resolve this issue, and to provide contact information for the Data Owner. If in fact the system has no Data Owner, you will be notified of this as well.

3. What if it the Data Owner is ambiguous?

Sometimes the identity of the Data Owner is not clear, or it is possible more than one individual could be the Data Owner. The information may be shared by two different systems; the system may function as an interface between other systems in the list; or elements of two different systems may be combined. It may not be possible to clearly assign a single individual as the sole Data Owner.

Again, the Office of the General Counsel should be contacted to resolve this issue. If there is a designated Data Owner, you will be provided with their contact information. If in fact the system has no Data Owner, you will be notified of this as well.

4. What if no Data Owner exists for a system, despite all efforts to find one?

A decision may be required about information disclosure where, despite all efforts, there is no assigned Data Owner for the system containing the information**.**

Should this be the case, you must first make a preliminary determination of the information's sensitivity, based on criteria supplied in the Information Protection Policy and other District policies. This determination should be made in the most conservative fashion. If there is any doubt about information sensitivity, choose the more sensitive category. For example, if you are not sure if the information should be Protected or if it should be Non-Public, choose Protected.

If the information is determined to be either Public or Non-Published Public, then the information may be disclosed to the requester.

If the information is determined to be either Non-Public or Protected, and there is no assigned data owner, the District Office of the General Counsel should be contacted immediately before releasing the information. The District Office of the General Counsel will coordinate with other offices to establish ownership.

In some cases, Non-Public or Non-Published information is requested under emergency conditions, where life or property is at immediate risk. Under these conditions, the information should be released; however the District Office of the General Counsel should be notified immediately of the circumstances.

Any request for District information that is part of legal proceedings (via subpoena, etc.) should be referred to the District Office of the General Counsel regardless of its sensitivity.

5. How does this policy affect my information security practices?

A system's sensitivity category and the Data Owner are important even if there are no pending requests to disclose information from the system. Information must be protected in a manner consistent with its assigned sensitivity as part of the normal procedures for handling information and managing systems.

All individuals who handle, manage, store, process, or communicate District information must handle that information consistent with its assigned sensitivity. Individuals having custodial responsibilities for hard copy records are responsible for knowing the information's sensitivity and ensuring that the hardcopy records are stored, handled, and disposed of consistent with the applicable District policies and procedures. Technical administrators are responsible for ensuring that the systems they control are secured according to District standards, based on the sensitivity of information being stored or processed.

6. Where can I go for further information?

You should call the Office of the General Counsel at (213) 241-7600 if you have any questions or concerns about how to handle protected information or if you have questions about the Data Ownership of specific information. In addition, if you have any information about possible violations of District information sensitivity policies, you should contact the Office of the General Counsel. You will not be penalized in any way for reporting such information.

If you have any questions about requirements for computer and network security, you should call the Information Security Coordinator at (213) 241-1343.

DISTRICT DATA OWNER MASTER LIST

APPLICATION	OWNER
Financial Information: - Transactions (G/L, etc.) - Summary reports - Budget - Position control	Chief Financial Officer
Payroll: - Time entry - Compensation - W2, reporting - Garnishments	Chief Financial Officer
Personnel: - Employee information	Chief Human Resources Officer Personnel Director
Transportation - Routing - Student use - DMV information	Director, Transportation Division
Student Information: - Enrollment - Home address, emergency contact - Grades - Test results - Disciplinary records - Medical - Instructional Programs	Chief Academic Officer Chief Executive Officer, Office of Educational Services Executive Director, Office of Data and Accountability
Facilities: - Project cost and schedule - Inventory - Maintenance - Disputes - Compliance audits	Chief Facilities Executive
Food Services: -Free and Reduced Status	Director, Food Services Division
Health Benefits and Claims	Director, Benefits Administration

APPLICATION	OWNER
Library Services: - Inventory - Patron use	Deputy Superintendent, Instructional Services
Third Party Claims: - Workers' Compensation case files	Division of Risk Management
Investigations - Compliance audits - Performance audits	Office of the Inspector General
Safety/Accident Investigations - Safety inspections - Test data	Office of Environmental Health and Safety
Information Technology: - Management and configuration - Application documentation - Help desk tickets - Telephone billing	Chief Information Officer
Procurement: - Purchasing - Contracts - Warehousing goods - Textbook management	Chief Procurement Officer

LAUSD EMPLOYEE
INFORMATION RESPONSIBILITY AGREEMENT

NAME: _____
Please Print

LAUSD EMPLOYEE #: _____

I have read and understand the District's policies regarding the security of District information and data. I agree to comply with each of the policies and procedures, and to maintain safe and secure work habits and to prevent the disclosure of sensitive information including but not limited to student, health care, and employee records.

I understand that violation of these policies may result in discipline up to and including termination.

_____ _____
Employee Signature Date