



**TITLE:** INFORMATION PROTECTION POLICY

**NUMBER:** BUL-1077

**ISSUER:** Office of the General Counsel

**DATE:** June 21, 2004

**POLICY:** It is the policy of the Los Angeles Unified School District (LAUSD) to protect sensitive information. The purpose of this Bulletin is to define the requirements for maintaining the security of information within and outside 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 requiring extreme care and sensitivity in handling, such as student or health care records. There are severe penalties when these records are mishandled and/or transferred to the wrong party and without consent, as specified below. This bulletin also addresses data ownership and responsibilities of data owners.

Note: Restrictions on information release are increasing and new laws to protect privacy are constantly being passed, and older ones 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:** This is a new policy.

**AUTHORITY:** This policy is established to address privacy rights contained within the Federal Education Rights and Privacy Act (FERPA), the Education Code, the Federal Health Information Portability and Accountability Act (HIPAA), the No Child Left Behind Act (NCLB), the USA PATRIOT ACT, and other Federal and State Laws.

**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 or federal law.

**ROUTING**  
All Employees  
All Locations



### Sensitivity Levels

District Information falls into one of four basic security levels:

1. Public Information: Information published on the District's public website or in other written 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.
3. Non-Public Information: Information that may or may not exist in the form requested, but by policy the District prevents it from publication. For example, the District will not reveal the results of evaluations of proposals prior to an award of an RFP and/or a recommendation to the Board. This would be an example of Non-Public Information.
4. Protected Information: Information that is protected by special laws. For example, student records, student and employee health records, and social security numbers, are each covered by specific privacy laws and rules. Please 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.

People outside the District seek information for a variety of reasons. Information in categories 3 and 4 should not be released. 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 write a letter or otherwise seek information under the California "Public Records Act." Whatever the sensitivity level of information, if a request for information has been made pursuant to the Public Records Act, that request should be directed to the Office of the General Counsel, Central Office Team at (213) 241-7600.



### **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. “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 purposes of determining the appropriateness of its release. For example, an individual student’s score on a standardized test is “owned” by the Assistant Superintendent of Planning, Assessment and Research, and not by the teacher who administered the test. A listing of current data owners is attached as 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 data owner must determine whether there is a legitimate reason for someone to access 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 being granted access is trained in their 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 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 school 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.

### **Role of LAUSD Information Security Coordinator (ISC)**

The District Information Security Coordinator (ISC) works within the Information Technology Division. The ISC is responsible for setting reasonable standards regarding the safety of data systems within the District and regarding the electronic transfer of sensitive information into or out of the District. The ISC can make recommendations for actions needed to comply with these standards in consultation with other branches, such as the Office of the General Counsel or the Office of the Inspector General or without such consultation, at his or her discretion. Employees who deal with vendors should let vendors know that they need to comply with ISC recommendations. All vendors providing, receiving or electronically exchanging data with the District shall cooperate with all requests for information made by the ISC. Any request made for a modification or alteration of a recommendation made by the District ISC may be made in writing to the Chief Information Officer.

In instances where the ISC reasonably believes that a data system inadequately protects records of a District student, employee or other sensitive information, and there is an urgent and compelling reason to protect that information from possible disclosure due to concerns of the security of the data system, the ISC with concurrence from either the Chief Information Officer, the Chief Operating Officer, the Chief of Staff, or the Office of the General Counsel may shut down the District data system involved until security issues are resolved.

### **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 (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, Central Office Team (213) 241-7600.
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, always obtain an executed copy of the Redislosure Agreement attached to this policy as **Attachment F**). The Redislosure Agreement places restrictions on a vendor's rights to the information and prohibits them from disclosing that information to others. 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 requested from time to time by student researchers (e.g. graduate students) seeking to access District information. No student/external researcher shall be allowed access to information without obtaining from the data owner a written consent form setting forth:



- (a) the specific data to which the researcher will have access,
- (b) a reasonable and specific period of time at the end of which consent to access will be discontinued,
- (c) the conditions regarding the researcher's publication of any information accessed during research and
- (d) a statement that the researcher will comply with all privacy statutes. The student researcher shall countersign the written consent. Student researchers shall not be given unlimited access or publication rights.

The data owner is responsible for granting only appropriate consent and enforcing compliance with the terms of the written consent and applicable privacy statutes. Fees may be charged to researchers if their research impacts staff resources. Fees may consist of any of the following:

- (a) hourly staff charges,
- (b) per page copying costs, and
- (c) data transmission costs (which may consist of a per student and/or per grade level fee). These fees shall be set by the Assistant Superintendent of Planning, Assessment and Research and may be changed from time to time to reflect the cost of the resources impacted by the researcher's activities. The Assistant Superintendent of Planning, Assessment and Research shall have discretion to waive such fees, if reasonable and appropriate.

### **Violations of Policy**

1. Violations of this Information Protection Policy may result in discipline, up to and including dismissal of personnel violating the policy.
2. Violations of certain portions of this policy may also be violations of state and/or federal law. Failure of personnel to comply with these policies could result in the employee being sued for a violation of privacy rights, or being prosecuted by a governmental agency charged with enforcing those rights.

### **RELATED**

**RESOURCES:** None



LOS ANGELES UNIFIED SCHOOL DISTRICT  
Policy Bulletin

---

**ASSISTANCE:** For assistance or further information please contact Richard A. Deeb, Office of the General Counsel at (213) 241-7600.

- ATTACHMENTS:**
- A. LAUSD FERPA POLICY**
    - A1. DISTRICT FORM FOR CONSENT TO RELEASE OF CONFIDENTIAL STUDENT INFORMATION**
    - A2. STUDENT EDUCATIONAL RECORD ACCESS LOG**
  - B. LAUSD HIPAA POLICY REGARDING STUDENT INFORMATION**
  - C. LAUSD EMPLOYEE RECORD POLICY**
  - D. DATA OWNER POLICY**
  - E. LAUSD EMPLOYEE INFORMATION RESPONSIBILITY AGREEMENT**
  - F. STUDENT RECORD CONFIDENTIAL AND RE-DISCLOSURES AGREEMENT**

**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 "Federal Education 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, 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: current and potential employers of District students, representatives of the news media, accredited colleges and universities, the PTA, Health Department, elected officials and the military (17 and 18 year olds only; name address and telephone only). If you have questions about whether Directory Information should be released call the Office of the General Counsel before releasing the information.

A student's parent or legal guardian (or, in some cases, a student) 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 request 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 individuals, 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 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, 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 with a legitimate educational interest in the requested information. Disclosure to any other District employee or representative for any other purpose (including for any use with 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 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, or 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.

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 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, must identify the party or class of parties to whom the records may be released, and must 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 age 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 to 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 OF 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: \_\_\_\_\_

UTime 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:** \_\_\_\_\_



## **LAUSD HIPAA POLICY**

### **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 not 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 if the student is under 18 years old, not emancipated or not legally permitted to consent to medical treatment, from the student's parent or legal guardian 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, MOTHER, GUARDIAN):**  
\_\_\_\_\_

**I HEREBY CERTIFY THAT I AM THE ABOVE STUDENT'S PARENT OR LEGAL GUARDIAN.**

**I HEREBY CONSENT 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 WITHDRAW 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 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 (in accordance with Board Rule 4511)
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 Board Rule 4511 and 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 Board Rule 4511 and 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, 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 (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 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	Business Manager
Student Information: - Enrollment - Home address, emergency contact - Grades - Test results - Disciplinary records - Medical - Instructional Programs	Deputy Superintendent, Instructional Services  Senior Deputy Superintendent, Educational Services  Assistant Superintendent, Planning Assessment & Research
Facilities: - Project cost and schedule - Inventory - Maintenance - Disputes - Compliance audits	Chief Facilities Executive
Food Services: -Free and Reduced Status	Business Manager
Health Benefits and Claims	Business Manager

<b>APPLICATION</b>	<b>OWNER</b>
Library Services: - Inventory - Patron use	Deputy Superintendent, Instructional Services
Third Party Claims: - Workers' Compensation case files	Office of the Risk Manager
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

## STUDENT RECORD CONFIDENTIALITY AND RE-DISCLOSURE AGREEMENT

The Los Angeles Unified School District ("**District**"), and the individual or entity identified as "Recipient" below ("**Recipient**") have entered or are planning to enter into an agreement or other arrangement that may involve Recipient's receipt of or access to certain student records and information concerning District students. The parties are entering into this Student Record Confidentiality and Re-Disclosure Agreement ("**Agreement**") in order to ensure proper treatment of any student record information that Recipient obtains or learns.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

### 1. Definitions.

a. "**Consenting Party**" means: (a) the natural parent, adopted parent, or legal guardian of each student or former student who is under the age of 18 years; and, (b) each student or former student who has attained the age of 18 years. Where a student's parents are divorced or legally separated, only the parent having legal custody shall be deemed to be the Consenting Party for purposes of this Agreement.

b. "**Student Record Information**" means any item of information (in any format, written, electronic, or other) that is directly related to an identifiable District pupil (current or former) and is maintained by the District or by a District employee in the performance of his or her duties.

2. Use of Student Record Information. Recipient will use Student Record Information only for the purpose of [Describe Project or enclose attachment describing Project] ("**Project**"), and will make no use of Student Record Information, in whole or in part, for any other purposes. Recipient will keep confidential all Student Record Information and will take all necessary steps to ensure the confidentiality of the Student Record Information. Recipient will only disclose Student Record Information in accordance with the terms of this Agreement and will make no other disclosure of Student Record Information at any time.

### 3. Re-Disclosure.

3.1. **Consent Required.** Recipient will only disclose Student Record Information to its employees having a need to know in connection with their Project responsibilities, and will not disclose any Student Record Information to any third party without first obtaining written consent to the disclosure from each Consenting Party for whom Student Record Information will be disclosed. Recipient will promptly provide the District with copies of any and all written consents that the Recipient obtains under this paragraph.

3.2. **Restrictions on Receiving Party.** In addition, any third party receiving Student Record Information from Recipient must agree in writing to all of the terms contained in this Agreement, and may only use Student Record Information for the performance of that third party's Project-related responsibilities.

3.3. **Exceptions.** Subject to this Agreement, recipient may disclose Student Record Information to third parties if, and only to the extent that, disclosure of the Student Record Information is otherwise permissible under applicable law or under any District privacy policy then in effect.

### 3.4. Access Log and Record Files.

Recipient will maintain an access log that records all disclosures of (or access to) Student Record Information. Entries in the

access log will identify the person(s) receiving access, the reason access was granted, the date, time and circumstances of disclosure, and all Student Record Information provided. The access log will be made available to the District promptly upon request.

4. Destruction of Information. Immediately upon completion of the Project, Recipient will destroy all Student Record Information that Recipient obtained or learned in connection with the Project. Upon the District's request, Recipient will promptly certify in writing that this destruction has occurred.

5. Required Disclosure. In the event that Recipient is requested or required by subpoena or other court order to disclose any Student Record Information, Recipient will provide immediate notice of the request to the District and will use reasonable efforts to resist disclosure until an appropriate protective order may be sought, or a waiver of compliance with the provisions of this Agreement granted. If, in the absence of a protective order or the receipt of a written waiver hereunder, Recipient is nonetheless, in the written opinion of its counsel, legally required to disclose Student Record Information, then Recipient may disclose that Student Record Information without liability hereunder, provided that the District has been given a reasonable opportunity to review the text of the disclosure before it is made and that the disclosure is limited to only Student Record Information specifically required to be disclosed.

6. No License. No licenses or other rights under patent, copyright, trademark, trade secret or other intellectual property laws are granted or implied by this Agreement. The District is not and will not be obligated under this Agreement to purchase from or provide to Recipient any information, service, or product.

7. Disclaimer. The Student Record Information is provided AS IS and without warranty of any kind, whether expressed or implied, including, without limitation, implied warranties of merchantability, fitness for a particular purpose or title. The District shall not have any liability or responsibility for errors or omissions in, or any decisions made by Recipient in reliance upon, any Student Record Information.

8. Remedies.

8.1. Injunctive Relief. The parties agree that Student Record Information is of a special character, such that money damages would not be sufficient to avoid or compensate the District, its employees, agents and students for any unauthorized use or disclosure thereof, and that injunctive and other equitable relief would be appropriate to prevent any actual or threatened unauthorized use or disclosure. This remedy may be pursued in addition to any other remedies available at law or in equity, and Recipient agrees to waive any requirement for the securing or posting of any bond. In the event of litigation to enforce any provision hereof, the prevailing party will be entitled to recover all costs, including its reasonable attorneys fees and costs, incurred in connection with the litigation.

8.2. Five-Year Bar. If the District determines, or is made aware of a determination by any other governmental agency, that Recipient has disclosed any Student Record Information in violation of this Agreement, or has maintained any Student Record Information in violation of this Agreement, then without prejudice to any other rights or remedies the District may have, the District shall be entitled to prohibit Recipient from accessing any Student Record Information for a period of five (5) years or more, as determined by the District in its sole discretion.

9. Indemnification. Recipient agrees to indemnify and hold harmless the District, its employees, agents, subcontractors, affiliates, officers and directors from, and defend the District against, any liability or expenses (including reasonable attorneys' fees and costs) arising out of or relating to: (a) any unauthorized or unlawful disclosure of Student Record Information by Recipient; or (b) any breach of this Agreement by Recipient.

10. Required Notice. Recipient shall notify the District immediately upon discovery of any unauthorized use or disclosure of Student Record Information, and will cooperate with the District in every reasonable way to assist the District in

regaining possession of the Student Record Information, mitigating the consequences of its disclosure, and preventing its further unauthorized use.

11. Governing Law; Venue. California law will govern the interpretation of this Agreement, without reference to rules regarding conflicts of law. Any dispute arising out of this Agreement will be submitted to a state or federal court sitting in Los Angeles, California, which will have the exclusive jurisdiction regarding the dispute and to whose jurisdiction the parties irrevocably submit.

12. Notices. All notices required or permitted to be given hereunder shall be in writing and shall be deemed given when delivered by hand, sent by courier or other express mail service, postage prepaid, or transmitted by facsimile, addressed to a party at the address set out by its signature below.

13. Waiver. No waiver of any term, provision or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, will be deemed to be or be construed as a further or continuing waiver of any such term, provision or condition or as a waiver of any other term, provision or condition of this Agreement.

14. Severability. If any provision of this Agreement is determined by any court of competent jurisdiction to be invalid or unenforceable, such provision shall be interpreted to the maximum extent to which it is valid and enforceable, all as determined by such court in such action, and the remaining provisions of this Agreement will, nevertheless, continue in full force and effect without being impaired or invalidated in any way.

15. Entire Agreement. This Agreement constitutes the parties' entire agreement with respect to the subject matter hereof and supersedes any and all prior statements or agreements, both written and oral. This Agreement may not be amended except by a writing signed by the parties.

IN WITNESS WHEREOF the parties have caused this Agreement to be executed by their duly authorized representatives.

**RECIPIENT**

\_\_\_\_\_  
Recipient Name

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Recipient Address

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

**THE DISTRICT**

Los Angeles Unified School District  
333 South Beaudry Avenue  
Los Angeles, California 90017

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date