



**LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN**

TITLE: App and Website User Agreements

NUMBER: BUL-6633.0

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

DATE: January 25, 2016

ROUTING
All Employees
All Schools

PURPOSE: The purpose of this Bulletin is to provide employees with the information necessary to properly navigate and accept or reject software application and website user agreements.

To protect employee and student data privacy, employees must only accept terms of service and use apps and websites that are in compliance with District policies and standards. Therefore, employees must thoroughly read the terms of service of an app or website, including its End User License Agreement (EULA) and Privacy Policy, prior to accepting the app or agreement terms and utilizing the app or website services.

A violation of this policy is considered a violation of the Responsible Use Policy (Bulletin No. BUL-999.11) and can result in loss of internet usage privileges and other administrative action as appropriate.

DEFINITIONS: App: An app, short for “application,” is software that allows you to perform specific tasks, such as download music, play games, or make purchases. Web apps or online apps are software applications that are available over the Internet. Mobile apps are software applications that run directly on mobile devices such as smartphones or tablets. Apps are commonly purchased from an app store, such as Google Play for apps that run on Android devices or the App Store for apps that run on Apple devices.

Clickwrap Agreements: Agreements in which users indicate their agreement to the terms of service by taking an affirmative action such as clicking an “I Accept” button or checking a box. Clickwrap agreements have been upheld by courts as enforceable contractual agreements.

Browsewrap Agreements: Agreements in which users are assumed to have accepted the terms of service simply by using the website. Often, no affirmative action is required. Browsewrap agreements have not always been upheld by courts as enforceable contractual agreements. Nonetheless, it is prudent for users to assume the agreements are enforceable and abide by the policies and procedures in this Bulletin.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information. PII includes, without limitation, name, address, parent and family names and addresses, social security number, and geolocation data.



LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY BULLETIN

Privacy Policy: A statement that discloses the ways a website gathers, uses, discloses, and manages a website user's data. State law requires a website operator that collects PII from users to conspicuously post its privacy policy on its website and to comply with that policy.

User: A person who uses an app.

PROCEDURES: The following procedures should be followed before utilizing an app or website that requires the user to enter into a clickwrap or browsewrap agreement:

1. **READ** the Terms of Service/EULA and Privacy Policy. If the terms are not immediately visible on a website, users should not assume that one does not exist. Instead, users should thoroughly check to see if the site has any explicit or implicit agreements prior to using the site's features.
2. Determine whether the website collects any PII from the user or requires the user to upload any PII. If PII is collected or uploaded, pay particular attention to the app or website operator's treatment of PII in the following areas:
 - a) Collection
 - b) Use
 - c) Re-disclosure
 - d) Retention
 - e) Destruction

Teachers: If the app or website requires the user to upload student PII, please contact the Office of General Counsel to ensure the appropriate protections are put in place to protect the PII. (See paragraph 7, below.)

3. Print out or scan and save the Privacy Policy and EULA to your files for future reference.
4. Beware of sites that collect PII for marketing or advertising purposes and share PII with third parties. Websites must disclose whether third parties may collect personal information about a user's online activities over time and across sites when the user visits the website.
5. If a website requires users to enter other sensitive information, such as birth dates, social security numbers, or credit card numbers, verify that the website utilizes a secure connection and encrypts sensitive or personal information. Sites using such technology will have a website address prefaced with <https://>. If the user does not trust that the website adequately describes its security measures



LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY BULLETIN

and handling of sensitive or personal information, the user should not utilize the website or its features.

6. If the site allows location tracking, look for a clear and conspicuous hyperlink in the privacy policy to an online location containing a description, including the effects, of any program or protocol the website follows that offers the choice to turn off tracking tools.
7. Federal and State laws restrict online businesses from collecting PII from students without parental consent, unless a specific exception applies. To determine whether an app or website directed toward students complies with data privacy laws, contact the Office of General Counsel.
8. If you become aware that any other App or website is collecting, using, or re-disclosing PII without user consent and in violation of law, please report the website to the Office of General Counsel.
9. If there is a cost associated with the app, check with the Procurement Services Division to determine whether you have delegated authority from the Board of Education to make the purchase before clicking "I Accept."

AUTHORITY: California Constitution, Article 1, section 1.

California Education Code, sections 49060- 49085

California Online Privacy Protection Act (CalOPPA), California Business & Professions Code (B&PC), section 22575.

Contracts with Third Parties for Digital Storage and Management of Pupil Records, Calif. Education Code section 49073.1

Privacy Rights for California Minors in the Digital World, Cal. B&PC, section 22580 et seq.

Student Online Personal Information Protection Act, Cal. B&PC section 22584, et seq.

Electronic Communications Privacy Act of 1986, 18 U.S. Code sections 2510-2522, 2701-2711, 3121,1367.

Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S. Code section 1232g

Children's Online Privacy Protection Act (COPPA), 15 U.S. Code section 6501 et seq.
Computer Fraud and Abuse Act of 1984, 18 U.S. Code section 1030



LOS ANGELES UNIFIED SCHOOL DISTRICT POLICY BULLETIN

Fteja v. Facebook Inc., (2012) 841 F. Supp. 2d 829

Nguyen v. Barnes and Noble Inc. (2014) 763 F.3d 1171

RELATED RESOURCES:

- Responsible Use Policy (RUP) for District Computer and Network Systems, Bulletin No. BUL-999.11, August 20, 2015
- Information Protection Policy, Bulletin No. BUL-1077.1, December 5, 2006
- Description of Security Standards for Networked Computer Systems Housing Confidential Information, Reference Guide No. REF-3757, June 13, 2007

CONTACTS:

For further information, please contact Chief Business and Compliance Counsel Gregory McNair at (213) 241-7600.

For Procurement questions, contact your Local District Buyer in the Procurement Services Division.