**TITLE:** Social Media Policy for Employees and Associated Persons

**NUMBER:** BUL-5688.2

**ISSUER:** Frances Gipson, Ph.D., Chief Academic Officer
Division of Instruction

Sophia Mendoza, Director
Instructional Technology Initiative

**DATE:** July 31, 2018

**POLICY:** The Los Angeles Unified School District Employees and all associated persons who work with or have contact with students are expected to follow all District policies when using social media as a form of communication. Under certain circumstances, the District has jurisdiction to discipline employees who violate rules of appropriate conduct which includes, but is not limited to, the use of social networking sites during or outside of work hours. Additionally, the District may not be able to protect or represent employees who incur legal action from a second party in response to the employee’s behavior on a social networking site.

**MAJOR CHANGES:** This revision replaces BUL-5688.1 of the same title, dated February 2, 2015 to reflect updated guidelines and definitions for District users while engaging in social media (Attachment A).

**PURPOSE:** The purpose of this updated bulletin is to provide policies and guidelines for social media communications between employees, students, parents and other associated persons; to prevent unauthorized access and other unlawful activities by District users online; to prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children’s Internet Protection Act (CIPA). While the District recognizes that during non-work hours employees and students may participate in online social media, blogs, and other online tools, District employees and associated persons should keep in mind that information produced, shared and retrieved by them may be subject to District policies and is a reflection of the school community.

**BACKGROUND:** The use of social media for instructional purposes can help augment instruction. However, when social media postings violate the law or District policies or create a substantial disruption to the school community and/or work environment, the administrator may have an
obligation to respond and take appropriate action, including but not limited to investigation and possible discipline.

GUIDELINES: I. SOCIAL MEDIA GUIDELINES FOR EMPLOYEES AND ASSOCIATED PERSONS

Many schools, offices and departments have their own websites and social media networks that enable staff to share school/work-related information (e.g., grades, attendance records, or other pupil/personnel record information) may be shared using only District-approved, secure connections and locations and only by authorized individuals. Confidentiality and security of privileged information regarding students or personnel must be maintained always.

All existing policies and behavior guidelines that cover employee conduct on school premises and at school-related activities similarly apply to the online environment in those same venues.

1. Keep personal social network accounts separate from work related accounts. When a student or minor wishes to link to an employee’s personal social networking site, redirect them to the school approved website. Accepting invitations to non-school related social networking sites from parents, students or alumni under the age of eighteen is strongly discouraged and, on a case-by-case basis, may be prohibited by the site administrator. (Code of Conduct with Students – Distribution and Dissemination Requirement) Office of Education Compliance.

2. Any employee or associated person engaging in inappropriate conduct including the inappropriate use of social media sites and applications during or after school hours may be subject to discipline.

3. Never post any personally identifiable student information including names, videos and photographs on any school-based, personal or professional online forum or social networking website, without the written, informed consent of the child’s parent/legal guardian and the principal.

4. Never share confidential or privileged information about students or personnel (e.g., grades, attendance records, or other pupil/personnel record information).

5. Users shall have no expectation of privacy regarding their use of District property, network and/or Internet access to files, including email. The District reserves the right to monitor users’
online activities and to access, review, copy, and store or delete any electronic communication or files and/or disclose them to others as it deems necessary. [Refer to BUL-999.12, Responsible Use Policy (RUP) For District Computer Systems] dated November 27, 2017.

6. Posting inappropriate threatening, harassing, racist, biased, derogatory, disparaging or bullying comments toward or about any student, employee, or associated person on any website is prohibited and may be subject to discipline.

7. Threats are taken seriously and are subject to law enforcement intervention, including but not limited to formal threat assessments. [Refer to BUL-5798.0, Workplace Violence, Bullying and Threats (Adult-to-Adult) dated July 16, 2012.]

8. District employees and associated persons are responsible for the information they post, share, or respond to online. Employees should utilize privacy settings to control access to personal networks, webpages, profiles, posts, digital media, forums, fan pages, etc. However, be aware that privacy settings bring a false sense of security. Anything posted on the Internet may be subject to public viewing and republication by third parties without your knowledge.

9. If you identify yourself online as a school employee or associated person, ensure that your profile and related content are consistent with how you wish to present yourself to colleagues, parents, and students. Conduct yourself online according to the same code of ethics and standards set forth in the Responsible Use Policy. It is recommended that you post a disclaimer on your social media pages stating, “The views on this page are personal and do not reflect the views of the Los Angeles Unified School District.”

10. Use of District logos or images on one’s personal social networking sites is prohibited. If you wish to promote a specific LAUSD activity or event, you may do so in accordance with the Office of Communications and Media Services guidelines.

11. Misrepresenting oneself by using someone else’s identity may be identity theft. It is advisable to periodically check that one’s identity has not been compromised.

12. During an emergency situation that impacts the employee’s worksite, the employee may post a general statement of wellbeing
II. EDUCATIONAL VALUE OF SOCIAL MEDIA

Technology is reshaping how we reach our students and how students interact with the world. For example, some teachers are using social media as an educational tool. Schools are using social media to launch anti-bullying campaigns, to share school news and events, to increase homework compliance and support, and to enhance classroom instruction. [Refer to https://achieve.lausd.net/iti for additional resources regarding social media and classroom instruction].

All social media interaction between staff and students must be for instructional purposes and must not include confidential information without parental and site administrator approval. [Refer to BUL 6399.2, Social Media Policy for Students, dated July 11, 2018].

The use of social media for instruction provides students the opportunity to engage in self-directed learning with differentiated paths to knowledge acquisition and processing. Students can use social media to catch up with course material as well as explore topics further. Social media also provides the opportunity for students to increase engagement with course content and to take advantage of peer learning. Using social media as an instructional tool will help augment students learning as well as help prepare them to be college and career ready.

When using social media for instructional purposes, the highest possible privacy settings must be utilized.

- The site administrator and parents must be notified of all classroom social media use.
- Additionally, the site administrator or designee shall have administrative access to the social media sites.
- If online commenting is enabled in an open site, the comments must be moderated and monitored daily for inappropriate language and content.

III. RESPONSIBILITIES OF DISTRICT EMPLOYEES AND ASSOCIATED PERSONS

A. All District employees and associated persons are expected to:

- Adhere to this Social Media Policy for Employees and Associated Persons.
LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

- Be familiar with and follow the guidelines and the provisions of this policy.

B. All District employees utilizing social media with students are expected to:

- Educate students about digital citizenship, which includes appropriate and safe online behavior, interacting with individuals on social networking websites, and cyberbullying awareness.
- Notify site/location administrator and parents (as appropriate) of all social media use.
- Provide site administrators with access to social media sites.
- Moderate and monitor comments daily posted either by staff or students.

IV. ADMINISTRATOR/DESIGNEE RESPONSIBILITIES:

A. In addition to those applicable duties listed in Section III, Administrators/Designees will

1. Distribute and communicate this Social Media Policy for Employees and Associated Persons to all employees and associated persons.

2. Investigate reported incidents of employee or associated adults’ misconduct or violations of appropriate conduct. [Refer to BUL – 999.12, Responsible Use Policy (RUP), dated November 27, 2017. For District Computer and Network Systems, Code of Conduct with Students – Distribution and Dissemination Requirement, please refer to the Education Equity Compliance Office.]

3. Postings of a serious nature may warrant additional reporting to Division and District Operations and the appropriate reporting agency:

   a. Threats (contact Los Angeles School Police Department (LASPD), School Operations, and Crisis Counseling and Intervention Services).

   b. Inappropriate or sexualized images of minors (contact both local law enforcement and LASPD).

   c. Child pornography (contact both local law enforcement and LASPD).
d. Raise a reasonable suspicion of child abuse (contact the appropriate Child Protective Services agency). [Refer to BUL-5798.0, Workplace Violence, Bullying and Threats (Adult-to-Adult), dated July 16, 2012. BUL-5799.0, Threat Assessment and Management (Student-to-Student, Student-to-Adult, dated July 16, 2012 and BUL-1347.3, Child Abuse and Neglect Reporting Requirements, dated August 19, 2016.

4. Inappropriate postings may be documented by taking and printing screen shots or downloading them as evidence. Evidence should be collected with the permission of the site administrator for the sole purpose of the investigative process and stored in a secured location. This evidence may be used in conference with the employee(s) or associated persons in question. Caution: Do not download or print images of minors or any content that may be considered child pornography. Law enforcement will gather evidence of child pornography, not a District employee.


6. The target of online harassment can request removal of objectionable postings by reporting the abuse to the Internet service provider or webmaster. Most social networking sites have the capacity to flag objectionable postings with “report abuse” button. The target should document the postings prior to their removal.

7. Monitor and follow-up to ensure that the inappropriate online behavior has stopped.

8. Refer to the appendix, Behavior Intervention Matrix.

B. Local District Superintendent should:

1. Communicate this Social Media Policy for Employees and Associated Persons to administrators and employees and associated persons.

2. Designate administrators to ensure the implementation of this policy.

C. Central Office Staff should:
1. Support this policy by assisting schools and worksites via trainings, consultation, and distribution of resources.

2. Align this policy with related District initiatives.

V. **GENERAL PROTOCOL FOR RESPONDING TO COMPLAINTS**

The following are general procedures for the administrator/supervisor to respond to any complaints:

A. Secure campus/office safety by ensuring all school site protocols are being followed.

B. Assure involved parties that allegations and complaints are taken seriously.

C. Investigate.

D. Take action to stop the behavior.

E. Request a factual written statement from the involved parties. Include witnesses if available.

F. Consult with the Local District, Staff Relations and other offices, as appropriate.

G. Document actions taken.

H. Implement disciplinary action as needed.

I. If appropriate, the victim may file a criminal complaint with law enforcement.

J. Continue to monitor and address inappropriate behaviors.

K. If appropriate, complete the Incident System Tracking Accountability Report (iSTAR).

L. Information about allegations of misconduct or investigations should be handled within the confines of the District’s reporting procedures and investigative process. The District will not tolerate retaliation against anyone for filing a complaint or participating in the complaint investigation process.
If the allegation is against one’s administrator or supervisor, that person’s supervisor shall respond to the complaint (Refer to BUL-5798.0, Workplace Violence, Bullying and Threats (Adult-to-Adult), Attachment D, Workplace Violence Complaint Form).

**AUTHORITY:** This is a policy of the Superintendent of Schools. The following legal authorities are applied in this policy:

California Education Code §44932 et seq. and California Penal Code §422 et seq.

**RELATED RESOURCES:**

- **BUL –999.12, Responsible Use Policy (RUP) For District Computer and Network Systems**, dated August 20, 2015
- **BUL–6399.2, Social Media Policy for Students**, dated July 19, 2018
- **BUL-1077.2, Information Protection Policy**, dated July 18, 2017
- **BUL-1347.3, Child Abuse and Neglect Reporting Requirements**, dated August 19, 2016
- **BUL-1893.1, Sexual Harassment Policy (Employee-to-Employee)**, dated August 1, 2005
- **BUL-2047.1, Responding to and Reporting Hate-Motivated Incidents and Crimes**, dated June 15, 2015
- **BUL-5159.7, Uniform Complaint Procedures (UCP)**, dated February 22, 2017
- **BUL-5212.2, Bullying and Hazing Policy (Student-to-Student and Student-to-Adult)**, dated November 26, 2014
- **BUL-5798.0, Workplace Violence, Bullying and Threats (Adult-to-Adult)**, dated July 16, 2012
- **BUL-044381.0, Protocols and procedures to Report, Reassign and Investigate Allegations of Employee Misconduct**, dated July 17, 2017
- **Employee Code of Ethics**, LAUSD Ethics Office, dated February 2003,
Los Angeles Unified School District Board Resolution, Respectful Treatment of All Persons, passed October 10, 1988

ASSISTANCE: For assistance and information, please contact any of the following offices:

LAUSD RESOURCES

Communications Office (213) 241-6766 - For obtaining approval to use District logos and general District communication

Crisis Counseling and Intervention Service, School Mental Health (213) 241-2174 or (213) 241-3841 - For threat assessments and mental health issues

Equal Opportunity Section (213) 241-7685 - For assistance with alleged adult-to-adult discrimination and sexual harassment complaints

Employee Relations (213) 241-6591 - For assistance with employee records and personnel files

Human Relations, Diversity and Equity (213) 241-8719 - For issues of bullying, cyber-bullying, conflict resolution, and diversity trainings

Information Technology Division (213) 241-4906 - For identifying and establishing appropriate educational websites

Instructional Technology Initiative (213) 241-5532 - For assistance with using technology as an educational resource

Los Angeles School Police Department (213) 625-6631 - For assistance with any law enforcement matters

Office of General Counsel (213) 241-7600 - For consultation regarding legal issues

School Operations Division (213) 241-5337 – For school operations and procedures concerning students and employees

Staff Relations (213) 241-6056 – For consultation regarding Employee assistance and guidance and/or disciplinary action.
DEFINITIONS

**Apps** are applications used to post media and are accessed primarily through mobile devices. Apps can often access the user’s pictures, personal information, and GPS location.

**Associated Persons** includes, but is not limited to, parents, parent-elected leaders of school committees, representatives and volunteers, consultants, contracted employees, walk-on coaches, child care/enrichment program providers, vendors and after-school youth services providers.

**Blogs** are personal websites that can serve as journals where a user can post a variety of content authored by the user and authored by others for public viewing.

**Confidential data** refers to District-related content such as (but not limited to) student personally identifiable information, grade and exam information, attendance data and behavior incidents.

**Cloud Computing**, otherwise known as ‘using the cloud,’ requires an Internet connection and is the practice of accessing files across multiple devices over the Internet.

**Digital Citizenship** is the practice of responsible engagement and respectful behavior online, which is demonstrated through the digital content a student posts.

**Digital Footprint** consists of an individual’s posting of content and profiles across multiple websites, applications, and other online platforms.

**Media Sharing Sites** are sites where users can store and share content such as video and pictures.

**Microblogs** are online spaces that allow users to post blog entries of limited length or characters.

**Social Networking Sites** are sites where users create and customize their own profiles with music, video, and other personal information in addition to connecting with other users.

**Tagging** is the practice of identifying and assigning information to a digital artifact such as a website, blog post, photo, video, or article for the purpose of easy identification, organization, aggregation, and searching. Tagging helps users find content they are looking for across online platforms.

**Wikis** are websites that allow visitors to make changes, contributions, or corrections.