Mt. Diablo USD
Draft Board Policy
Revised: 12/2/13

All Personnel **BP _____**

SOCIAL MEDIA AND TECHNOLOGY USE POLICY

The Mt. Diablo Unified School District ("District") is committed to providing a safe and secure learning and working environment for its students and employees. The District encourages positive relationships between students, employees and associated persons. There is, however, a distinction between being supportive of students and the real or perceived breach of confidentiality or misconduct. Employees and all associated persons who work with or have contact with students are expected to follow all District policies, including the following: Employee Responsible Use Policy; Video Monitoring Policy for Employees; Administrative Regulation for Social Media and Technology Use Policy; and Bring Your Own Device Policy, when using social media as a form of communication.

Purpose

The purpose of this policy is to:
1. Provide policies and guidelines for social media communications between employees, students, and employees to parents;
2. To prevent unauthorized access and other unlawful activities by District users online;
3. To prevent unauthorized disclosure of or access to sensitive information; and
4. To comply with the Children's Internet Protection Act (CIPA).

While the District recognizes that during non-work hours employees 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 on the school community.

Background

Social media has many benefits but when social media postings violate the law or District policies or create a substantial disruption to the school community and/or work environment, the District administrator may have an obligation to respond and take appropriate action, including, but not limited to, investigation and possible discipline. Under certain circumstances, the District has jurisdiction to discipline employees who violate rules of appropriate conduct, which may include 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 in a social networking site.

Definitions

Blogs are updated personal journals with reflections, comments, and often hyperlinks provided by the writer intended for public viewing.

Digital Publishing Site is an Internet personal publishing service that provides products and services for consumers to preserve their digital photos or films, such as Shutterfly, Flickr and YouTube.

A Mobile Device (also known as a hand held device, hand held computer or simply hand held) is a small hand held computing device, typically having a display screen with touch input and/or a miniature keyboard, and weighing less than 2 pounds. Apple, HTC, LG, RIM, and Motorola are just a few examples of the many manufacturers.

Podcasts are audio broadcasts that have been converted to MP3 or other audio file format for playback in a digital music player.

Social Media also referred to as social networking, is a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.

Social Networking Websites are websites where users can create and customize their own profiles with photos, videos, and information, such as Facebook, GooglePlus, Habbo and other social networking sites.

Tags (Tagging) are keywords assigned to a webpage for the purpose of easy identification, organization, aggregation and searching. Most social media sites allow users to tag the content they share online such as articles, photos, videos or blog posts. Tags help users find content they are looking for through social media sites and other online platforms.

Wikis are websites that allow the creation and editing of any number of interlinked web pages via a browser using a simplified markup language or a text editor.

Social Media Protocol for Employees

Many District schools, offices and departments have their own websites, learning management systems, and social media networks that enable staff to share school/work-related information. Confidential or privileged information about students or personnel (e.g., grades, attendance records, or other pupil/personnel record information) may be shared only on District-approved secured connections by authorized individuals to authorized persons.

SOCIAL MEDIA POLICY FOR EMPLOYEES (con't.)

All existing policies and behavior guidelines that cover employee conduct on the 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 18 is strongly discouraged.

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

3. Never post any identifying 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. Students, including teaching assistants ("TAs") must not be given access to employees' district-issued, or the employee's own, computer to enter grades or attendance.

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

5. Staff should use security settings and encryption where appropriate.

6. **Users should 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, store, or delete any electronic communication or files and/or disclose them to others as it deems necessary, and in accordance with Federal, State, and local regulations.**

7. Posting inappropriate threatening, harassing, racist, biased, derogatory, disparaging or bullying comments toward or about any student or employee, on any website, learning management system, and social networking website is prohibited and will subject an employee to discipline.

8. Threats are taken seriously and are subject to law enforcement intervention, including but not limited to, formal threat assessments.

9. District employees 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.

10. If you identify yourself online as a school employee, 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 Agreement. 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 Mt. Diablo Unified School District."

11. Use of District logos or images on one's personal social networking sites is prohibited. If you wish to promote a specific District activity or event, you may do so in accordance with the Office of the Superintendent.

12. Misrepresenting yourself by using someone else's identity may constitute identity theft or fraud. It is advisable to periodically check that your identity has not been compromised.

Mobile Device Protocol for Employees

A. District mobile devices are intended solely for employee use in job-related activities.

B. Confidential data should never reside on a mobile device unless authorized by the Superintendent or designee.

C. Software: No software of any kind shall be installed by anyone on any District mobile device, such as a laptop computer or tablet, without prior approval from your administrator or the Technology and Information Services department. Unauthorized software may interfere with proper functioning of the device. Software laws must be strictly adhered to.

D. Never cancel an antivirus or automatic operating system update. These are crucial and are for your protection. Note: viruses and malware can compromise your data even if your mobile device is encrypted.

E. Hardware: No hardware additions or changes to any District computer shall be done by any employee other than District technicians.

F. Service: All service must be performed by Technology and Information Services technicians, site technicians or authorized technicians from the company that provides warranty service. It is expressly forbidden for you to let any friend, neighbor, family member, outside agency, yourself or anyone else attempt to repair or configure your mobile device.

G. We recognize that access to some data off District property is becoming more common. Employees must take reasonable steps to safeguard confidential District data when accessing it in any location.

Telephone and Mobile Phone Protocol for Employees

A. Telephones and cell phones are services meant to contact parents, agencies, vendors, institutions, and government officials. When using these services, your comportment should be business-like and professional. Private use of phones should be kept to a minimum. Employees are responsible for any charges incurred when using District phones for purposes not related to their job duties.

B. Cell phones should never be used while operating a vehicle (use hands-free). Pursuant to California Law, no employee operating a District vehicle and/or transporting students or other staff shall text while driving.

C. No sexting of any kind can be done on District-owned equipment, including servers.

Email Protocol for Employees

Email is a widely-used tool for conducting business in the District. Many employees report receiving "too may emails" or emails that are confusing. To assist with those concerns, employees should keep in mind when using District email:

A. Use the "Subject Line" to clearly summarize your message. Properly titled messages help people organize and prioritize their email. Avoid generic subject lines. If you are starting a new conversation, don't reply to an old email that has a different subject.

B. Be cautious with the "CC (Carbon Copy)" function. Overuse simply clutters inboxes. Copy only people who are directly involved.

C. Use the "Reply All" button carefully. You may end up broadcasting your response to many more people than intended and create work for those who do not need to see your response.

D. Use the "BCC (Blind Carbon copy)" when addressing a message that will go to a large group of people, so recipients won't have to see a huge list of names. By using BCC, each recipient sees only two emails addresses, theirs and yours. In addition, if recipients use "Reply All" to your message, it won't automatically go to any addresses in BCC.

E. All District Email shall contain the following confidentiality notice which shall appear beneath the employee's signature and contact information

> "CONFIDENTIALITY NOTICE: This electronic mail transmission, including any attachments, may contain confidential information only for use by the

intended recipients. Any privileges or confidentiality afforded under the law are not waived by virtue of this having been sent by electronic mail. Unless you are the addressee (or authorized to receive messages for the addressee), you may not use, copy, disclose, or distribute this message (or any information contained in or attached to it) to anyone. If you received this transmission in error, please notify the sender by reply e-mail or by telephone and delete the transmission. Thank you.

F. **Remember that District email is not private. Users should not have an expectation of privacy regarding their use of District email. The District reserves the right to monitor employees' email and to access, review, copy, store or delete any electronic communication or file and/or to disclose them to others as it deems necessary, and in accordance with Federal, State, and local regulations.**

G. Keep messages brief and to the point. Concentrate on one subject per message whenever possible.

H. Use a signature that includes contact information to ensure that people know who you are.

I. Watch formatting. Do not overuse colors or graphics in your message, because not everyone uses an email program that can display the. Examples of these include "cute" pictures, non-standard fonts and colorful page backgrounds. Also, using all CAPITAL LETTERS in and email appears to be shouting.

J. Direct personal email to your home email account. District email resources are intended solely for District-related business.

K. Don't send chain letters, virus warnings, junk mail, or jokes. Always check a reputable antivirus web site or the Technology and Information Services Department before sending out an alarm.

Legal Reference:
(California Education Code §44932 et seq.)
(California Penal Code §422 et seq.)

Related Resources:
BP 1312.3 Uniform Complaint Procedures
BP 4040 Employee Use of Technology
BP 5131.2 Bullying
BP 6163.4 Student Use of Technology
BP 3513.1 Employee Use of Cell Phones
BP ___ Employee Responsible Use
BP ____ Video Monitoring Policy for Employees
AR ___ Social Media and Technology Use
BP ____ Bring Your Own Device

Policy approved: _____

MT. DIABLO UNIFIED SCHOOL DISTRICT
Concord, California