The Marysville Joint Unified School District Student Social Media & Acceptable Use Policy

Introduction
Marysville Joint Unified School District (MJUSD) recognizes that access to technology in school gives students and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21-century technology and communication skills.

To that end, we provide access to technologies for student use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus.

- The network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- We make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.
- Users of the network or other technologies are expected to alert school staff immediately of any concerns for safety or security.

In order for students to utilize District technology resources, both the District's parent(s)/guardian(s) and the student must sign and acknowledge receipt of the policy and sign it, indicating the student agrees to comply with the policy. The District will not grant access to information technology until this signed form is received.

Technologies Covered
MJUSD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, MJUSD will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies
All technologies provided by MJUSD are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Training
A student will not receive access to information technology until he/she has participated in an orientation or training course with a MJUSD faculty member as to proper behavior and use of the network.

Web Access
MJUSD provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. In order to comply with both CIPA and its implementing rules, the District will make a reasonable effort to filter out material and pictures that constitute: (a) obscenity; (b) child pornography; or (c) material harmful to minors, for computers that are accessed by minors. These efforts include, by way of illustration and not limitation, the following precautions:

a. Blocking access by minors to inappropriate material on the internet.
b. Preventing unauthorized access, including so-called "hacking," and other unlawful activities by minors online.
c. Preventing unauthorized disclosure, use, and dissemination of personal information regarding minors.
d. Restricting minors' access to materials harmful to them.

Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert a school staff member or submit the site for review.

No Expectation of Privacy
Users have no expectation of privacy while using District information technology. District staff may monitor or examine all system activities to ensure proper use of the system.

Email
MJUSD has created email accounts for all students in grades K-12 to allow for collaborative sharing using the District's student safe email system. The District uses a private software application for this purpose. These accounts will be used at school for school related projects but may be used outside of school for personal email by students with their parents' permission. The accounts will allow access to the wealth of collaborative tools available to students and teachers once these accounts are assigned. No student will be assigned an email account until this signed form is received.

The email naming convention will include graduation year, part of the student's name, and a part of their ID number. For example, John Smith graduation in 2029 with an ID number of 123456 would have an email address of 29jsmi456@mjusd.k12.ca.us. This email address will be considered the student's official MJUSD email address until such time as the student is no longer enrolled in MJUSD.

Parents may opt their students out of email use if they opt the student out of all use of District online technologies.

Email accounts should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the District policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived. In addition, in the normal course of system administration, system administrators may have to examine activities, files, and email to gather sufficient information to diagnose and correct problems within system software or hardware.

Users of student email are strictly prohibited from accessing files and information other than their own. Like all District technologies, access to and use of student email is considered a privilege given at the discretion of MJUSD. The District reserves the right to access student email accounts, including current and archival files of user accounts, when there is reasonable suspicion that unacceptable use has occurred. The District maintains the right to immediately withdraw the access and use of student email when there is reason to believe that violations of law or District policies have occurred. In such cases, the alleged violation will be referred to the Principal for further investigation and adjudication.

Social / Web 2.0 / Collaborative Content

Recognizing that collaboration is essential to education, MJUSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. (See also the section on Social Media Responsible Use Guidelines, below.)

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy

MJUSD may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to school staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including use of the school network, may be monitored.

Personally-Owned Devices

Students may use personally-owned devices (i.e. laptops, tablets, smartphones, cell phones, etc.) at any time during school hours—unless such use interferes with the delivery of instruction by a teacher or staff or creates a disturbance in the educational environment. Any misuse of personally-owned devices may result in disciplinary action. Therefore, proper network etiquette and adherence to the Acceptable Use Policy should always be used. In some cases, a separate network may be provided for personally-owned devices.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert a school staff member. Do not attempt to remove the virus yourself or download any programs to help remove the virus. In order to maintain security for District technology resources, students must abide by the following directives:

- If you identify a security problem, notify the classroom teacher, site administrator, or District system administrator at once.
- Never demonstrate the problem to other users.
- Never use another individual's account without written permission from that person.
- All use of the system must be under your own account if one was provided.
- Never engage in intentional conduct designed to circumvent any District security devices or software including, by way of illustration and not limitation, firewalls and/or filtering or blocking programs.
- Never download software (including, by way of illustration and not limitation, games and instant messaging programs), hardware, attachments, graphics, photos, documents or any other files to District computers unless otherwise authorized by a teacher, administrator, or system administrator.

Any user identified as a security risk will be denied access to the information technology system.

Updating

The information technology service may occasionally require new registration and account information from you to continue the service. You must notify the information technology system administrator of any changes in your account information.

Downloads

Users should not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites and only for educational purposes.

Network Etiquette

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- Users should also remember not to post anything online that they wouldn’t want parents, teachers, or future colleges or employers to see. Once something is online it can be shared and spread in ways you never intended.

Plagiarism

- Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet.
- Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

- Users should never share personal information, including phone number, address, social security number, birthday, or financial information over the Internet without adult permission.
- Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.
- Users should never agree to meet someone they meet online in real life without parental permission.

Staff will closely supervise students while using online services and may ask instructional assistants and student aides to assist this supervision.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.

- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use
I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally-identifying information about myself or others.
- Agree to meet someone I meet online in real life without parental permission.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Social Media Responsible Use Guidelines
The District may encourage teachers, students, staff, and other school community members to use social networking/media as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience.

Social networking/media includes, by way of illustration and not limitation: Twitter, Facebook, Blogspot, Word Press, YouTube, Instagram and other networks, websites and blogs which allow online communication/interaction between users. If you have a question regarding whether a particular application, program, or website constitutes social networking/media, please seek assistance from a teacher or administrator.

While social networking is valuable, there are some risks involved in its use. In the social media world, the lines are blurred between what is public or private, personal or professional. The following guidelines are specific to social networking/media. You must follow them any time you utilize social networking/media for MJUSD or school-related purposes. These must be applied in conjunction with the acceptable use rules contained in this document, and all acceptable use rules apply to social networking/media.

When using social networking, you must: Use good judgment

- We expect you to use good judgment in all situations.
- You must know and follow all District policies, regulations, and procedures regarding use of technology, as well as all applicable disciplinary policies.
- Regardless of your privacy settings, ***assume that all of the information you have shared on your social network is public information, and treat it as such.***
- Users are responsible for their own behavior, and will be subject to discipline for violations of these guidelines where appropriate, including violations of District policies regarding cyberbullying and related misconduct.
- Be respectful.
- Always treat others in a respectful, positive, and considerate manner.
- Social networking/media should be utilized during school hours only during times when it is allowed by the teacher or other authorized adult.

Be responsible and ethical

Unless you are specifically authorized to speak on behalf of MJUSD or your school as a spokesperson, you should state that the views expressed in your postings, etc. are your own. Only discuss matters that are within your area of responsibility.

- Be open about your affiliation with MJUSD.
- Be a good listener.
- Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly, and to share feedback.
- Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc.
- Always do at least as much listening and responding as you do “talking.”
- Report any violations of this policy immediately.

Don’t share the following:

Confidential information

- Do not publish, post, or release information that is considered confidential or not public. If it seems confidential, it probably is. Online “conversations” are never private. Do not use your birth date, address, and cell phone number on any public website.
- Private and personal information.
- To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.
- NEVER give out or transmit personal information of students, parents, or school staff.
- Don’t take information you may receive through social networking (such as email addresses, customer names, or telephone numbers) and assume it’s the most up-to-date or correct.

- Always respect the privacy of MJUSD and school community members.

<u>Please be cautious with respect to</u>:

Images

- Respect brand, trademark, copyright information and/or images of MJUSD or school (if applicable).
- You may use photos and video (products, etc.) that are available on MJUSD's or school's website.
- It is generally not acceptable to post pictures of students without the expressed written consent of their parents.
- Do not post pictures of others without their permission.

Other sites

- A significant part of the interaction on blogs, Twitter, Facebook, and other social networks involves passing on interesting content or linking to helpful resources. However, MJUSD is ultimately responsible for any content that is shared. Don't blindly repost a link without looking at the content first.
- Pay attention to the security warnings that pop up on your computer before clicking on unfamiliar links. They actually serve a purpose and protect you and MJUSD.
- When using Twitter, Facebook, and other tools, be sure to follow their printed terms and conditions.

And if you don't get it right…

- Be sure to correct any mistake you make immediately, and make it clear what you've done to fix it.
- Apologize for the mistake if the situation warrants it.
- If it's a MAJOR mistake (e.g., exposing private information or reporting confidential information), tell an administrator immediately so the school or MJUSD can take the proper steps to help minimize the impact it may have.
- If you are uncomfortable with any social media interactions which have occurred, immediately report the issue to a teacher or administrator.

Limitation of Liability
MJUSD makes no warranties of any kind, whether expressed or implied, for the service it is providing. MJUSD will not be responsible for damage or harm to persons, files, data, or hardware. Damages include loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or your errors or omissions. While MJUSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. MJUSD specifically disclaims any responsibility for the accuracy of information obtained through its services. Further, MJUSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Students accept responsibility for compliance with this policy and for reporting any misuse of the information technology network to the classroom teacher, site administrator, or district Technology Department. Misuse is defined as any violation of this policy. The District's system administrator(s) (operating under the aegis of the school board and the district office) will decide what constitutes appropriate use. Their decision is final. The system administrator may deny access at any time deemed necessary.

Use of the information technology system is a privilege and not a right. Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases.
- Notification to parents in most cases.
- Detention or suspension from school and school-related activities.
- Legal action and/or prosecution.

STUDENT

I understand and will abide by the provisions and conditions of this policy. I understand that any violations of the above provisions may result in disciplinary action, the revoking of my user account, and appropriate legal action. I also agree to report any violations of this policy or any other district policy or policies regulating information technology resources to the classroom teacher, site administrator, or District system administrator. All the rules of conduct described in this policy apply when I am on the network.

____
(Student Printed Name)

____
(Student Signature)

____
(Date)

PARENT/GUARDIAN

All students must have the signature of a parent/guardian who has read this policy. As the parent/guardian of this student, I have read this contract and understand that it is designed for educational purposes. I understand that it is impossible for the District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the network. I also agree to report any violations of this policy or any other District policy or policies regulating information technology resources to the District system administrator. I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission to issue an account for my child and certify that the information contained on this form is correct.

____
(Parent Printed Name)

____
(Parent Signature)

____
(Date)