



Moraga School District

1540 School Street

Moraga, CA 94556

Julie C. Parks, Ed. D., Superintendent

Acceptable Use Policy Internet Use and Network Access Policy (Students)

Internet access is coordinated through a complex association of government agencies, and regional and state networks. The smooth operation of the network depends upon the proper conduct of all students who must follow guidelines established by the school district that provides access to this worldwide network. In compliance with state and federal regulations, the Internet is filtered and monitored for all users. Via our Internet filter, Securely, parents are given opt-in access to student online activity at school, as well as at home when on District loaned Chromebooks.

Terms and Conditions of this Agreement

Acceptable Use – Student use of the Internet must be in support of education and research, and consistent with the educational objectives of the Moraga School District.

1. **Privileges** – The use of the Internet is a privilege, and unacceptable use will result in limited access or cancellation of those privileges. The principal, faculty, and staff at any school site may request that student access to the Internet be denied, taken away, or suspended for violations of this agreement.
2. **Network Behavior** – You are expected to follow generally accepted rules of Internet/Network behavior. This includes, but is not limited to using appropriate language and keeping private all personal information including name, home address, phone numbers, age, and/or photographs of yourself or others. Student email accounts are provided at school for grades 2nd-8th grades for educational use only. Students are not to access personal email unless requested by a teacher to support instruction.
3. **Unacceptable Use** – Transmission of any material in violation of any U.S. or State law is prohibited. This includes, but is not limited to: copyrighted material; threatening, harassing, or obscene material; or material protected by trade secrets. Use of district resources for commercial activities, product advertisement, or political lobbying is prohibited.
 - **Communication & Social Media:** Students are prohibited from accessing chat rooms, instant messaging, or any social networking and media-sharing platforms, regardless of whether they are accessed via a web browser or a standalone application. This includes, **but is not limited to**, Snapchat, X/Twitter, Instagram, **TikTok**, **Discord**, or any emerging equivalent services, **as well as the unauthorized use of communication features within educational applications.**
 - **Content Creation:** Students shall not view, create, or transmit inappropriate material (including content that is sexually explicit, violent, or promotes illegal acts). Students are prohibited from posting personal web pages or threatening/cyber-bullying comments to any digital forum, **private message group**, or website regardless of privacy settings and using district resources.
 - **Media Capture:** Students are prohibited from **taking, creating, or modifying** video, still digital pictures, or **AI-generated media** while at school and transmitting or posting them to the internet or social media without explicit staff authorization.
 - **Unauthorized Disclosure (PII):** Students shall not disclose, use, or disseminate personal identification information (PII)—including, **but not limited to**, name, address, email, telephone number, or Social Security number—of themselves, other students, staff members, or any other person.
 - **Harassment:** The use of any digital tool to threaten, intimidate, harass, or ridicule any person is strictly prohibited. This includes the use of AI to generate, modify, or distribute non-consensual media, "deepfakes," or impersonations of any student or staff member. **This applies regardless of whether the action occurs on a district-owned or personally-owned device, or whether the action occurs on or off-campus**, if the action creates a substantial disruption to the school environment or interferes with the rights of others.

4. **Artificial Intelligence (AI) and Academic Integrity** – Student use of Generative AI must support the educational objective of developing original critical thinking. The following rules apply to all AI interactions:

- **Privacy & Data Security:** Sharing confidential or personally identifiable information (PII) of themselves or others with any AI system is strictly prohibited. Adjusting privacy settings on any AI application is prohibited unless explicitly directed by staff.
- **Authorization Requirement:** Students may only use Generative AI tools when a teacher has provided explicit permission for a specific assignment or task. Unauthorized use of AI to complete assignments is considered a violation of academic integrity.
- **Mandatory Attribution:** Any work that includes AI-generated ideas, text, or images must be clearly disclosed and cited. This includes documenting the specific AI tool used and the nature of the assistance provided (e.g., brainstorming, outlining, or proofreading).
- **Content Protection:** Students are prohibited from uploading district-owned instructional materials, including teacher-created worksheets, assessments, or copyrighted curriculum, into any external AI model without prior authorization.
- **Fact-Checking:** Because AI systems may produce inaccurate or biased information, students are responsible for verifying any AI-generated facts against trusted, non-AI secondary sources.
- **Human-Centered Work:** AI should be used as a supplemental tool for the production process; however, the final submitted work must reflect the student's own unique analysis, reflection, and synthesis of information.
- **Final Accountability & Non-Delegation:** *The student is considered the sole "author of record" and is fully responsible for the accuracy, integrity, and appropriateness of all work submitted, regardless of the tools used. Use of AI does not absolve the student of responsibility for plagiarism or factual errors. Furthermore, the use of AI to impersonate others, create "deepfakes," or generate non-consensual altered media is strictly prohibited and will be treated as a severe disciplinary violation.*

5. **Use of Portable Media** – CDs, portable USB flash drives, and any other portable device are to be used only to transport school work between the district and home computers. No additional programs, tools, or games are to be used or installed on district computers.

6. **Personally Owned Devices** - If a student uses a personally owned device to access district technology, the student shall abide by all applicable board policies, administrative regulations, and this Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

7. **System Integrity and Unauthorized Use** – Any unauthorized or malicious use of district technology, network resources, or software will result in disciplinary action, which may include the immediate termination of student accounts and/or loss of device privileges. Unauthorized use **includes, but is not limited to:**

- **Circumventing Security:** Attempting to bypass or "hop" district web content filters through the use of Virtual Private Networks (VPNs), proxy servers, "unblocker" websites, or any other hardware/software tools, **including but not limited to browser extensions or specialized search queries**, regardless of the student's intent or the nature of the content accessed.
- **Unauthorized Access & Phishing:** Attempting to gain access to, or "phish" for, another user's computer, data, or login credentials. This includes using another person's account even with their expressed permission.
- **Possession of Exploits & Specialized Hardware:** Being in possession of, saving to any drive (local or cloud), or utilizing **including, but not limited to:** "hacking" tools, packet sniffers, exploits, unauthorized encryption software, **or hardware devices designed to intercept or interfere with wireless signals (e.g., signal jammers or unauthorized wireless injectors).**
- **Network Interference & Automated Tools:** Intentional damage or attempting to damage district hardware; creating or attempting to spread computer viruses, ransomware, or malware; **the use of automated scripts, "bots," or data-scraping tools;** or engaging in activities that deliberately degrade network performance.
- **Vandalism:** Altering, deleting, or "defacing" any district web pages, digital files, or the work of other users.
- **Credential Sharing:** Sharing, trading, or selling network passwords, multi-factor authentication codes, or account

access information with any other individual.

- **Unauthorized Testing:** Probing or "testing" district security or vulnerabilities without explicit, written authorization from the District Technology Department. Finding a security vulnerability does not grant permission to exploit or further investigate that vulnerability.

8. **Use of Information** - The Moraga School District makes no guarantee of any kind, whether expressed or implied, for the service it is providing. Network storage areas may be treated like school lockers. Network and school administrators may review files and communication to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers or cloud storage will be private. Plagiarism is strictly prohibited by students, which includes copying from other students, copying from Internet sources, submitting papers purchased online, submitting work written or completed by others, and submitting the work of tutors, parents, siblings, or friends as one's own work.

If a student becomes aware of any security problem (including, but not limited to, a cyberattack, phishing, or any compromise of the confidentiality of any log in or account information), or misuse of district technology, the student shall immediately report such information to the teacher or other district personnel.

Any violation of the provisions as set forth in this Acceptable Use Policy can result in termination and/or limited access to the MSD network. I have discussed and explained this Acceptable Use and Internet Safety Policy with my child. I have discussed with my child their responsibility for appropriate network and Internet use while at school.