



Responsible Use Agreement (Students)

In addition to the Morgan Hill Unified School District (MHUSD) Acceptable Use Agreement, this document outlines specific Responsible Use Agreement details to which students enrolled at Morgan Hill Unified School District will be required to adhere.

Google Apps for Education (GAFE)

MHUSD students will be accessing the following applications from Google Apps:

- **Gmail** – A webmail service that combines the best features of traditional email with Google's search technology; includes email, chat, and video conferencing.
 - Email will be archived in the event of disciplinary/subpoena purposes.
 - The presence of the student's legal guardian must be acknowledged for any student/teacher, student/student video conferences through Google Video hangouts.
 - Student username/email addresses will be generated by MHUSD Technology Dept. and will use the domain @students.mhusd.org.
 - Student accounts will be identified by avatars created at www.weeworld.com to maintain student anonymity. No pictures portraying the students will be allowed.
- **Google Drive** – Web-based application to create and edit documents, spreadsheets, and presentations. Store documents online and access them from any computer.
 - Students and teachers will collaborate through shared documents.
 - Documents will not include a student's personal info (e.g. phone number, address, etc...)
 - Students will be identified by their assigned alphanumeric username.
 - No pictures in which the student can be identified will be allowed.
- **Google Calendar** – Web-based time-management application that is part of Google Apps.
 - Students will be using Google to view dates for field trips, assignment due dates, meetings, etc...
 - Students will use Google Calendar to track tasks, scheduled appointments, create reminders, etc. to assist them in managing their time.
 - Google Calendar allows students to see their teacher's availability.
- **Google Sites** – Online system for creating a website that is as easy as editing a document.
 - Students will be using Google Sites for an electronic portfolio.
 - A template will be created to maintain student anonymity, protecting student identity.
 - A generic title will be used for the portfolio, including only the student's first name.
 - Posted material must be appropriate for education purposes connected to curriculum.
 - No pictures in which the student can be identified will be allowed.



Google's Commitment to Educational Domains

- Google Apps for Education is ad-free – MHUSD's content is not processed by Google's advertising systems.
- Protection of the intellectual property on the servers is critically important to

Google.

- Google Apps brings you the latest technologies and some of the best practices for user privacy.
- Apps content belongs to the individual users at your school. Not Google.
- We don't look at your content. Google employees must have explicit permission even for troubleshooting.
- We don't share your content. Google does not share personal information without your consent.
- We sometimes scan content for spam filtering, anti-virus protection, or malware detection.

I understand that by participating in Google Apps for Education, the only information about my child will be collected and stored electronically is their username and password. I have read the privacy policies associated with use of Google Apps for Education

(<http://www.google.com/a/help/intl/en/edu/privacy.html>)

Unacceptable Uses of MHUSD Technology

MHUSD reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the school, students, employees, network or computer resources, or (2) that expend school resources on content the school in its sole discretion determines lacks legitimate educational content/purpose, or (3) other activities as determined by school as inappropriate.

The following are examples of unacceptable uses of MHUSD technology and may be grounds for student discipline up to and including suspension and expulsion.

- Transmitting on or through the network any material that is unlawful, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, or federal law, statute or regulation;
- Criminal activities that can be punished under the law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming or "chain letters"; spreading viruses;
- Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Causing harm to others or damage to their property, such as:
 - Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
 - Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;



- Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- Using any computing device to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws;

- Users may not attempt to circumvent user authentication or security of or jeopardize services to any host, network, or account. Examples include:

- Accessing data the user is not expressly authorized to access;
- Probing the security of the District's network and the networks of others, password sniffing; IP spoofing;
- Install network or server equipment not authorized by the District;
- Bypassing District proxy services;
- Using another's account password(s) or identifier(s);
- Interfering with other users' ability to access their account(s);
- Disclosing anyone's password to others or allowing them to use another's account(s).

- Using the network or Internet for Commercial purposes:

- Using the Internet for personal financial gain;
- Using the Internet for personal advertising, promotion, or financial gain;
- Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Penalties for Improper Use

Misuse of District technology may lead to disciplinary including the possible loss of technology use, suspension, expulsion and/or legal action. Technology use is a privilege, not a right. Individual schools sites will apply disciplinary action based upon the seriousness of each violation. School administrators, or designees, shall retain the right to review the content of any district-issued student account or device.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

I have read, understand, and agree to abide by the provisions of the Responsible Use Agreement of Morgan Hill Unified School District.

Student Signature: _____ **Date:** _____

Print Student Name: _____

Guardian Signature: _____ **Date:** _____

Print Guardian Name: _____