

Monroe-Gregg School District Acceptable Use Policy (2020-2021)

Introduction

Monroe-Gregg recognizes that access to technology in school gives students 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 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff 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 Monroe-Gregg network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained indefinitely.
- 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.
- Monroe-Gregg makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from the use of school technologies.
- Students are held accountable for actions on educational platforms used within the classroom *even* in cases that students are using a personal device at home.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Monroe-Gregg may provide Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more.

In some cases, Monroe-Gregg will use Zoom for remote learning- By signing this AUP, it is understood that I have read through the [Zoom Privacy Policy](#), specifically paying attention to the

following bullet points:

- We do not use the data we obtain from your use of our services, including your meetings, for any advertising. We do use the data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com. You have control over your own cookie settings when visiting our marketing websites.

- We are particularly focused on protecting the privacy of K-12 users. Both Zoom's Privacy Policy (attached) and Zoom's K-12 Schools & Districts Privacy Policy are designed to reflect our compliance with the requirements of the Children's Online Privacy Protection Act (COPPA), the Federal Education Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA), and other applicable laws.

As new technologies emerge, Monroe-Gregg 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.

Monroe-Gregg balances the educational value of online resources with any privacy concerns that they may present. On occasion, staff may leverage necessary online educational resources that collect basic information, such as a student's first and last name and email address, based on the provider's policy and practices of safeguarding such information. Student Google accounts will also be used to access other educational tools as deemed necessary for instruction by the school. Please note that Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes. According to [Google's Privacy Policy](#), they will not share personal information with companies, organizations, or individuals outside of Google unless one of the following circumstances applies:

- A parent or guardian provides consent
- The individual is an employee of Monroe-Gregg School District
- For external processing
- For legal reasons

By acknowledging receipt of the student handbook, it is understood that Monroe-Gregg will create and maintain a G Suite for Education account for my child.

Usage Policies

All technologies provided by the district 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.

Internet Access

Monroe-Gregg 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. Web browsing may be monitored and web activity records may be retained indefinitely.

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 district protocol to alert an IT staff member or submit the site for review.

Email

Monroe-Gregg may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. Students may not access personal email accounts on district devices.

Monroe-Gregg utilizes G Suite for Education and will provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more. Students will use their G Suite accounts to complete assignments, communicate with their teachers, sign in to their Chromebooks, and learn 21st-century digital citizenship skills. In compliance with the Children's Online Privacy Protection Act (COPPA), we want to notify you of your parental rights related to any data collected about your student while using G Suite or other educational online tools.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from the unknown or untrusted origin; should use appropriate language; 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 will be monitored and archived.

Social / Collaborative Content

Recognizing the benefits collaboration brings to education, Monroe-Gregg may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging will be monitored. Users should be careful not to share personally-identifying information online. When using social platforms for the classroom, the same rules apply regardless of using a school device in the classroom or a personal device outside the classroom.

Mobile Devices Policy

Monroe-Gregg may provide users with Chromebooks or other devices to promote learning 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 IT staff immediately. Users will be financially accountable for any damage resulting from negligence or misuse.

The use of school-issued mobile devices off the school network will be monitored.

Personally-Owned Devices Policy

Students should keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during school hours—unless in the event of an emergency or as instructed by a teacher or staff for educational purposes.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from IT staff. 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 your IT department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

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.

Users may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Digital Citizenship

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's out there—and can sometimes 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

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.

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.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, trolling, 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.
- 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, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- 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:

- Violate any local, state, or federal statute.
- Use school technologies in a way that could be personally or physically harmful.
- Use district technology to access, create, store, or distribute inappropriate images or content including but not limited to pornographic, obscene, abusive, illegal, or sexually explicit content.
- Use district technology to access dating or gambling sites.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- 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.
- 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, 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.

Limitation of Liability

Monroe-Gregg will not be responsible for damage or harm to persons, files, data, or hardware. While Monroe-Gregg employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Monroe-Gregg will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of the network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Other actions as deemed appropriate by the school administration
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

(Printed Name)

Monroe-Gregg School District

Acceptable Use Policy

(Signature)

(Date)