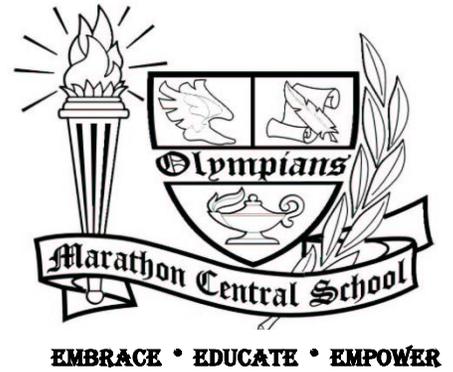**Laptop and G-Suite Handbook**

I) Procedures and Information for Students and Parents

Marathon Central School District would like to offer 7th and 8th grade students the opportunity to utilize an assigned laptop at school for one to one use.   This initiative prepares students for a globally interconnected and evolving world that experiences rapidly changing technological advancements. This will help fulfill the mission and vision of the district to embrace, educate, and empower all learners.

1) Receiving Your Laptop (Grades 7-8)

Parent/Guardian Agreement

At the beginning of the school year, prior to receiving a district computer to use at school (grades 7 through 8), parent(s)/guardian(s) are required to sign the district Laptop Acceptable Use Agreement form.

Distribution

Our technology team will roll out the assigned laptops to students at the beginning of each school year and only after the majority of students and parents have read and have signed-off on the agreements.

2) Returning Your laptop to the cart at the end of each day (Grades 7-8)

Ongoing Policy

The 7th and 8th grade teachers and/or technology staff will regularly check to see that students return their laptops to the assigned carts at the end of the day. Any reported missing laptop is immediately investigated. If a student discovers that their laptop is missing, they should report it to the technology department immediately.

Transferring/Withdrawing Students

The technology department will make sure exiting students have left their laptop in an acceptable condition in the cart upon departure and will remove this asset from the charging carts to be recycled into the hands of any new student. Missing laptops are still the responsibility of the student until the asset has been properly reclaimed by the technology department. If the laptop is not found in good condition, the exiting student will be held accountable and charged for the repair or replacement of the computer. Unpaid fines and fees of students leaving district may be turned over to a collection agency if not paid in a timely manner. If necessary, the District may also file a report of stolen property with the local law enforcement agency.

3) Taking Care of Your Laptop

Students are responsible for the general care of the laptop they have been issued by the

district. In the event of damage, loss, or inoperability, a temporary device will be made available until the primary device is repaired or replaced. Students should never leave their computers unattended except locked in their locker or other building / district designated secured areas.

General Precautions

- No food or drink should be near laptop's.
- Cords, cables, and removable storage devices must be inserted and removed carefully.
- Laptops should not be used in classroom with the power cord plugged in when the cord may be a tripping hazard.
- Laptops must remain free of any writing, drawing, stickers, labels or permanent personalization.
- Heavy objects should never be placed on a laptop.

Carrying Laptops

- Always transport laptops with care.
- Use 2 hands when moving a laptop around.

Screen Care

- The laptop screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure.
- Do not put pressure on the top of a laptop when it is closed.
- Do not store a laptop with the screen open.
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

Asset Tags

- All laptop's will be labeled with an individual student number.
- Number labels may not be modified or tampered with in any way.

Alterations

- Any alterations to laptops are not allowed.
- Removing or tampering with any of the components of the laptop is not allowed.

4) Using Your Laptop at School

Students are expected to bring their laptop's to all classes unless specifically advised not to do so by their teacher.

Laptop's being repaired

- A loaner computer may be issued to students until their laptop is repaired.

- A student borrowing a loner computer must sign it out and will be responsible for any damage or loss of the loaned device.

Charging Laptop's

- Students should charge their laptop's at school in the designated location every evening.

Backgrounds and Themes

- Inappropriate media may not be used as laptop backgrounds or themes. The presence of such media will result in disciplinary action.

Sound

- Sound must be muted at all times unless permission is obtained from a teacher.

- Headphones may be used at the discretion of the teachers.

- Students should have their own personal set of headphones for sanitary reasons.

Printing

- Students will be encouraged to digitally publish and share their work with their teachers and peers when appropriate.

- Printing is available in most of the classrooms and the library.

Logging into a Laptop

- Students will log into their laptop's using their school issued user name and password.

- Only Marathon accounts are able to log in to district-issued laptop's.

- Students should never share their account passwords with others.

- Students should not log onto another person's laptop with their username and password.

Managing and Saving Your Digital Work with a Laptop

- Student work may be stored in Internet/cloud based applications and can be accessed from any computer with an Internet connection and most mobile Internet devices.

- Students should always remember to save frequently when working on digital media; G Suite applications will auto-save every 4-6 seconds while connected to the internet.

- The district will not be responsible for the loss of any student work.

Operating System and Security

- Students may not use or install any operating system on their laptop or physically alter the laptop in any way.

Updates

- Updates are completed by the technology department over summer breaks.

5) Student Safety and Content Filtering

The district utilizes an Internet content filter that is in compliance with the federally mandated

Children's Internet Protection Act (CIPA). All laptop's, regardless of physical location, will have all Internet activity protected, managed, and monitored by the district per policy.

Aristotle Keylogging & Lightspeed Filtering

The district uses the Aristotle keylogging application to track and monitor laptop usage. Lightspeed is used to filter all Internet content. This service allows the district to filter content anywhere and anytime on any network. No existing system can provide perfect filtering but it can be very effective when coupled with classroom and parent oversight. Students caught manipulating or trying to bypass filtering and keylogging software may be subject to losing access to their device and school Internet access on other school devices.

Student Safety Responsibilities

- Students are not allowed to post personal contact information about themselves or other people. This includes names, addresses, and phone numbers.

- Students should never meet personally with someone whom they have met online without their parent's approval and participation.

- Students will tell their teacher or another school employee about any message or file they receive that is inappropriate or makes them feel uncomfortable.

- Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a student provide his or her password to another person.

6) Software

G Suite (Formerly Google Apps for Education)

G Suite is available at home, the library, or anywhere with Internet access. School staff will monitor student use of G Suite when students are at school. Parents/guardians are responsible for monitoring their child's use of G Suite when accessing programs from home. Students are responsible for their own behavior at all times.

Microsoft Store Apps and Extensions

- Students are allowed to install appropriate Microsoft Store Apps from the Microsoft Store on their own laptop.

- Students are responsible for the Microsoft Store apps they install on their laptop's. Inappropriate material will be removed and may result in disciplinary action.

- Some Microsoft apps will be available to use when the laptop is not connected to the Internet.

- Students that need a Microsoft App or Extension but are unable to install it should go to the technology department (room 201) to have it installed.

7) Laptop Identification

Records

The district will maintain a log of all laptop hardware that includes the laptop serial number, and student name/ID number of the student assigned to the device.

Users

Each student will be assigned a laptop for the duration of his/her time at school. It is the intent of the District to have each student be assigned a computer that they will use for their entire 7-8 school career. Students will <u>not</u> be assigned a different computer each year.

8) Lost or Damaged Laptop's

Consequences for losing or damaging a laptop will be handled on a case-by-case basis by building and/or district administrators.

- Any damaged laptop must be brought to the technology department to be assessed.
- Any damage will be put on file.
- The district's technology department will assess the damage to determine repair requirements, if needed, or delay the repair to a suitable future date to which the student is still responsible for.
- When repair costs are actually incurred, the technology department will submit a fair claim to the principal's office to be pursued with the student and parent(s)/guardian(s).

Estimated Costs (subject to change)

The following are estimated costs of commonly damaged Laptop replacement parts:

- Replacement - $250
- Screen - $50

Payments for damages can be remitted to:

Marathon Central School District
1 Park St.
Marathon, NY 13803

9) Policy

Acceptable Use (Privacy and Safety)

G Suite (formerly known as Google Apps for Education) is primarily for educational use. Students may use G Suite for personal use subject to the restrictions below and additional school rules and policies that may apply.

Students may use G Suite tools for personal project but may not use them for:

- Unlawful activities
- Commercial purposes (running a business or trying to make money)
- Personal financial gain (running a website to sell things)

- Inappropriate, sexual, or other offensive content
- Threatening another person
- Harassment or bullying
- Actions which are a violation of the Dignity for All Students Act (DASA)
- Misrepresentation of the District, staff, or students. G Suite sites and groups are not public forums; they are extensions of classroom spaces where student free speech rights may be limited.

Access Restriction - Due Process

Access to G Suite is considered a privilege afforded at the discretion of the District. The District maintains the right to immediately withdraw the access and use of G Suite 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 or principal's designee for further investigation and account restoration, suspension, or termination. As a party of the agreement with Google, the school also reserves the right to immediately suspend any user account suspected of inappropriate use. Pending review, a user account may be terminated as part of such action. In addition, further consequences may be applied per the student code of conduct.

Privacy and G Suite

Students have no expectation of confidentiality or privacy with respect to any usage of a district-issued laptop, district G Suite accounts or other related district network asset, regardless of whether its use is for district-related or personal purposes other than as specifically provided by law. The district may, without prior notice or consent, log, supervise, access, view, monitor, or record use of student laptop or G Suite account at any time for any reason related to the operation of the district. By using a district-issued laptop or district G Suite account, students agree to such access, monitoring, and recording of their use.

Monitoring Software

School staff may use monitoring software that allows them to view the screens and activity on student laptop's.

Student Privacy Pledge Signatory

Google is a Student Privacy Pledge Signatory, which holds school service providers accountable to:

- Not sell student information
- Not behaviorally target advertising
- Use data for authorized education purposes only
- Not change privacy policies without notice and choice
- Enforce strict limits on data retention
- Support parental access to, and correction of errors in, their children's information
- Provide comprehensive security standards
- Be transparent about collection and use of data.

There are NO ADS in G Suite.

G Suite does not collect or use student data for advertising purposes or create advertising profiles.

- Upon student departure, students are encouraged to back up their files and data to their own personal accounts. The district will suspend student accounts upon graduation or departure from the district.

Administrative Audit

Upon request from district administration, the technology department will provide a complete and unedited audit log of all administrative access, changes or monitoring of student accounts on the G Suite administrative console and/or the Aristotle administrative console.

10) Appropriate Uses and Digital Citizenship

School-issued laptops should be used for educational purposes and students are to adhere to the Acceptable Use policy and all of its corresponding administrative procedures at all times.

While working in a digital and collaborative environment, students should always conduct themselves as good digital citizens by adhering to the following:

1. **Respect Yourself**. I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will be appropriate and act with integrity.

2. **Protect Yourself**. I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.

3. **Respect Others**. I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites: I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.

4. **Protect Others**. I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.

5. **Respect Intellectual property**. I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.

6. **Protect Intellectual Property**. I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and

refrain from distributing these in a manner that violates their licenses.

Digital Citizenship (Advice for All)

Treat others well. When making a post on a forum or web page, be kind. Everyone will see what you write, so think before you type. Be careful with what you say about others and yourself.

Respect the rights of copyright owners. Copyright infringement occurs when an individual reproduces a work without permission that is protected by copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether they can use a work, he or she should request permission from the copyright owner.

Students have First Amendment rights to free speech. Your rights can be limited in school. If you post something via a school web page that disrupts the learning environment in your school, your right to free speech may be limited. A school or school district has the right to limit student speech that disrupts the learning process.

11)   Cyber-Safety and Cyber-Ethics

In an effort to educate faculty, students and parents, the district will offer ongoing cyber-safety and cyber-ethics curriculum. We will be offering parent technology workshops and ongoing support to help facilitate this process.

Child Internet Protection Act (CIPA)

The school is required by CIPA to have technology measures and policies in place that protect students from harmful materials including those that are obscene and pornographic. This means that student email is filtered. Mail containing harmful content from inappropriate sites will be blocked.

-- CIPA - http://fcc.gov/cgb/consumerfacts/cipa.html

Children's Online Privacy Protection Act (COPPA)

COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. By default, Google advertising is turned off for G Suite users. No personal student information is collected for commercial purposes. This permission form allows the school to act as an agent for parents in the collection of information within the school context. The school's use of student information is solely for educational purposes.

-- COPPA - http://www.ftc.gov/privacy/coppafaqs.shtm

Family Educational Rights and Privacy Act (FERPA)

FERPA protects the privacy of student education records and gives parents rights to review student records. Under FERPA, schools may disclose directory information (name, phone, address, grade level, etc...) but parents may request that the school not disclose this information.

- The school will not publish confidential academic records (grades, student ID #, etc...) for public viewing on the Internet.

- The school may publish student work and photos for public viewing but will not publish student last names or other personally identifiable information.

- Parents may request that photos, names and general directory information about their children not be published.

- Parents have the right at any time to investigate the contents of their child's email and G Suite files.

 -- FERPA - http://www2.ed.gov/policy/gen/guid/fpco/ferpa

Dignity for All Students Act (DASA)

New York State's Dignity for All Students Act seeks to provide a safe and supportive environment free from discrimination, intimidation, taunting, harassment, and bullying on school property, on school buses, and/or at school functions.

 -- DASA - http://www.p12.nysed.gov/dignityact/

12) Contract

Students will be issued a laptop which will be used while at school and stored in a designated secure location. Students are responsible for picking up their assigned computer each morning and returning it to its designated slot at the end of each day. All laptops that are not working properly must be turned in to the technology department immediately, and not returned to the cart in the charging carts.