Coleman Middle School Device Usage Guidelines

All Coleman Middle School (CMS) students must adhere to the Responsible Use of Electronic Media (RUEM) when using their devices or the GCPS network. The primary goal of GCPS and CMS is to ensure that every student is provided with a safe and secure environment both in and out of the classroom when working with Technology to enhance their educational experience. The RUEM also serves as an honor code for all uses of Technology. It is CMS' expectation that all students will make good choices when using the CMS issued device. The RUEM also serves as a practical guide for students to reference when using Technology to support their instructional needs. The RUEM is also a reminder that the primary focus of the 1:1 device deployment is to support instruction. All CMS devices are on loan to the students for the academic year and are to be used solely as an instructional tool. CMS retains the right to collect and / or inspect the Computer at any time and to alter, add or delete installed software or hardware.

Because each student will be issued a device for instructional use during the school day, students **will not be allowed** to use their own devices (cell phone, laptop, I-pod, I-pad, etc.) between arrival and dismissal. Consequences will be issued to students who do not comply with this school policy. Teachers will inform both students and parents in advance if phones can be used during a specific activity (i.e. taking pictures on a field trip, etc). Should parents need to communicate with their child during the school day, they need to call the appropriate grade level office.

The following Sections provide specific guidelines for students to follow. Not adhering to these guidelines can result in the loss of devices and network privileges, as well as disciplinary action(s).

Section I: CMS Device Equipment Provided

Every student is issued a device for instructional purposes; the device must be turned in and charged at the end of each school day. At no time should any student take a GCPS issued device off campus unless instructed to do so by a faculty/staff member. It is the student's responsibility to maintain the integrity of these items over the course of the year at CMS.

Section II: Device Care & Safety

The following guidelines are provided to help keep your device in good repair. If you need further information or assistance, please contact the CMS Technology team for support.

- When transporting your device, you must close the device. It is best practice to hold the device in between the chest and forearm to protect it against damage.

- Report any loss or damage to the device or peripherals immediately to the CMS Technology Department. Damage includes missing keys on keyboard, cracked LCD display or damaged device hinges, broken CD/DVD drive, frayed AC power cords, any type of liquid spill

on the device or the device submerged under water.

- Never leave your device unattended at CMS or any other public location.

- According to the RUEM, each student is responsible for all parts of the device, including peripheral equipment (mouse, cables, power adapters, etc.).

- When asked to return your device to your technology team for repairs or maintenance, please do so immediately.

- Avoid eating or drinking near the computer, as food can damage the keyboard and the electronics directly under the keyboard. At school, please finish your breakfast or lunch before accessing your device.

- Do not install unapproved software on the device. Your TST and/or LSTC will work with you to identify software that has been reviewed for instructional purposes by your school's Instructional Media Committee (see GCPS Policies and Procedures P.IFAA) and technically evaluated by the Division of Information Management and Technology.

- The device has been issued to you personally. Ultimately you will be held responsible for any damage (up to the current replacement cost of the device).

- You are required to change your network password(s) when you receive the device. Do NOT share your passwords with anyone. The principal and/or a designee assigned by the principal may also keep a list of student passwords for support purposes.

Section III: CMS Appropriate Use of Student Technology & Hardware

ACCESS IS A PRIVILEGE - NOT A RIGHT! Inappropriate use will result in a cancellation of these privileges as well as possible assignment of disciplinary action consistent with the policies and procedures of Gwinnett County Public Schools. Specific behaviors may result in disciplinary actions that are automatically escalated to Level 2 and/or the loss of GCPS technology. Such behaviors include the following uses of a CMS issued computer:

- Downloading and / or installing any applications, executable files or software not specified by CMS or GCPS.

- Using any means including a proxy anonymizer to bypass the GCPS Proxy server on /or off-campus.

- Downloading and/or viewing pornographic images and / or videos.

- Uploading or downloading audio files using GCPS technology without prior written consent of GCPS.

- Downloading music files, including purchased-services sites (iTunes, Wal-Mart, Amazon Music, etc.) without prior written or verbal consent from a CMS Faculty Member.

- Transferring music to or from MP3Players, iPods, USB drives, SD Cards or other digital storage devices to computer(s).

- Using a GCPS computer to access storage devices (external hard drives, USB drives, SD Cards, etc) containing gaming software for playing on the GCPS computer.

- Bullying and threatening other individuals using GCPS technology devices to upload, read, and / or participate in defamatory behaviors via forums, e-mail, chatting, social networking sites, blogging sites, etc.

- Unauthorized use of an AC power supply not provided by CMS including the use of another student's AC Power Supply.

- Taking any part of the device apart and putting it back together.

- Downloading and installing any type of desktop themes other than Microsoft Certified.

- Downloading and installing any type of computer games, regardless of the development platform, such as Flash or runtime files.

- Downloading and installing any type of computer skins to change the look of the desktop or any other computer settings.

- Uploading games to the shared network to host multi-game playing.

- Using a USB device, SD card or other external device to install malicious software and or executable scripts on a fellow student's device.

- Running any type of command scripts to interfere with the integrity or performance of another student's device.

- Downloading and or installing executable that allow the user to quickly minimize or hide a running application through a series of "hot keys" or mouse clicks.

Additionally, the capturing of video, digital stills or audio clips of students, teachers, and others using CMS/GCPS technology or personal technology without CMS permission can result in severe disciplinary action, especially since this violates Federal privacy regulations. Under no

circumstances are CMS/GCPS computers to be used to post images and / or video clips of themselves, classmates, teachers, or staff without prior permission of CMS/GCPS, regardless of the technology used to post such video or audio files. There may also be legal ramifications for the sending, receiving, creation, or dispersal of slanderous or threatening email, instant messages or blog comments.