MECS Technology Acceptable Use Policy (TAUP)

OBJECTIVE
Integrate the benefits of technology in the learning environment while teaching wise stewardship and biblical principles.

RESPONSIBILITY and APPLICATION
General Aspects:
MECS promotes the use of technology recognizing it serves the school's vision to be recognized as a Christian educational institution committed to the formation of global citizens who show love for God and others, exercising transformational leadership. MECS shall provide students with Internet access and computer access to enhance, enrich, and facilitate learning and communication. Elementary and Secondary School's access to technology devices will be through a BYOD (Bring your own device) program. Preschool will make use of school iPads and may bring their devices upon teachers' request.

This TAUP is designed to establish clear guidelines for all students who have been granted access to electronic devices and outlines how technology can be used in positive and honorable ways. Technology access for students is a privilege, not a right. With privilege comes responsibility and as a condition of use, students and parents are required to read and abide by the guidelines outlined in the Acceptable Use Policy.

In order to assist students in the use of technology resources, the school will do everything it can to ensure that students access the resources appropriately. This includes providing:
- an Internet connection that is protected by filtering software. Filtering blocks for sites that are objectionable for content, language, or a variety of other things that the school has defined as inappropriate, such as releasing personal information.
- a password protected school Google Apps account for students. While Google Apps is web-based and accessible via the Internet from home or school, students agree to use this account for school purposes only. Google accounts will be deleted when the student leaves MECS.
- Students will receive instruction in conducting online research via the Web and other online sources and taught to manage the information found. Expectations will be clearly defined and students will be aware of what constitutes a violation.

Technology Acceptable Use: The technology user shall follow all applicable School policies and procedures, including this Acceptable Use Policy ("TAUP"), and the Student Code of Honor. Users are held responsible for their actions when using the Internet, the network, and any action done under his/her login name. These policies, procedures, and rules are applicable whether students are online or in the physical school building.

It is expected that Technology is used as a tool to facilitate learning and communication. Some acceptable uses are:
- Research
- Organization of materials
- Brainstorming
- Composition
- Note-taking
- Instructional software and Internet activities
- Projects
- Correspondence
- Discussion Forums
- Electronic Collaboration
- Instruction
- Educational APPs

Teachers' Guidelines for Technology Use

Teachers should:
- Actively supervise student use of the Internet.
- Make every effort to ensure that students are directed to sites with only age- and topic-appropriate material.
- Model appropriate use of the Internet through their use of technology in the classroom.
- Explore a website before directing students to the website.
- Assign research projects that require students to access the Internet under direct, one-on-one adult (i.e., teachers, parents, etc.) supervision.

●Model the skills needed to search for information within an area of study, to filter information for credibility and worth, and to recognize areas of inappropriate information sources or access.

Entering 10th grade, teachers play a more advisory role with upper secondary students' use of technology.
- Appropriate modeling and teaching concerning Internet safety and technology stewardship are still practiced in the classroom, but more responsibility is placed on the student as he makes choices but still operates within the conditions of the TAUP.

Use of Devices
General regulations:
- While the student is on campus, personal technology devices (such as laptops, iPads, e-readers, or any other tablet or device with Internet capability and wireless accessibility) may only be used for educational purposes with permission.
- Students may use their personal electronic devices during assessments under supervision.
- Students may not use personal devices or school resources to text or use online chats or instant messaging at any time, including any posting on social network sites during school hours.
- Personal technology devices are not to be used for calculator work during assessments, measurement conversion assistance, idle web surfing, game playing, music sharing or listening, or personal communication while on campus.
- All phones should be kept off in the Principal's office. These are not to be accessed in or out of class without permission.
- Headphones should not be used unless directed by a teacher to use for educational needs.
- All communication to parents by a student or to students by a parent should be handled through the school office.

While using the network students are expected to:
- Be polite and courteous.
- Use appropriate language.
- Always log out when you are finished at a computer, laptop or tablet.
- Assume any material posted on the Internet is public and not private.
- Share resources.
- Understand that technology will break or not work correctly at all times.
- Maintain a Christian testimony while posting, blogging, emailing, surfing the web, and maintaining social networks.

Students are expected to refrain from:
- Using the network for any illegal activity, accessing any inappropriate sites, financial gain or initiating any financial transactions or non-permitted activities such as downloading personal programs or software.
- Posting rude or inappropriate messages/material through MECS Internet. (wearing, using vulgarities, or using any language inappropriate for a school setting, posting personal and/or confidential information) This includes comments that could be considered defamatory against MECS or its staff or material authored or created by another without his or her consent.
- Disclosing personal information to websites or people through the Internet unless deemed necessary for educational purposes.
- Posting personal communications without the author's consent or posting information containing information not meant to be made public.
- Accessing or vandalizing the data of another user, or using the login, password, account of another user – with or without that user's permission. This includes invading the privacy of individuals by reading mail that belongs to others without their permission.
- Attempting unauthorized access to resources, including any action to get around the filter installed on a computer with Internet access.
- Using resources resulting in plagiarism. (refer to Academic Honesty Policy)
- Participate in cyberbullying, which is defined as the use of electronic media to support deliberate, repeated, and hostile behavior by an individual or group with the intention of physically or psychologically intimidating others.

●Use resources wastefully (e.g. bandwidth, file space, paper, and ink/toner) or fail to respect the MECS resource limits.
- Gain unauthorized access to resources or entities.
- Sending, receiving, displaying, or accessing inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal materials.
- Encouraging the use of or promoting the sale of controlled substances or drugs.
- Any attempt to harm or destroy data of another user, the network, any technology equipment, or any of the agencies or other computer network services that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.
- Redistributing a copyrighted program or copyrighted material without the express written permission of the owner or authorized person or as provided by the fair use exception. This includes uploading and downloading of materials.
- Leaving an account open or unattended.
- Accessing another's data storage device.
- Altering computer equipment as set up by the system administrator.
- Transmission of any material in violation of any RD regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening material, obscene information and/or pictures, vandalizing material such as computer viruses, and trade secrets.
- Sharing electronic files or copying another's online work and calling it your own (plagiarism/cheating)
- Vandalizing resources and equipment.
- Downloading applications without teacher permission.
- Gaming or social networking.
- Video surfing and viewing video or music programs, channels, websites, or apps without permission from a teacher. Any permission obtained is for completing a school assignment only.
- Sharing information, you wouldn't want parents, pastors, 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.
- Image searching using unfiltered search engines such as google images or using social media such as Facebook or Instagram as a searching tool.
- Not reporting any malicious or inappropriate material that is offensive, unsafe, or violates policy.
- Violating the spirit of MECS Mission Statement.

Use of School email
The MECS Google Domain is a private learning management tool including a set of intelligent apps such as: Gmail, Docs, Drive, Calendar, and Classroom designed to promote critical thinking, creativity, collaboration and communication between students and teachers in an instructional setting.

MECS provides students a Google Domain account, which includes email, as an educational tool, and in fulfilling their academic and school-sponsored extracurricular activities. A Google Domain account is not private and may be monitored and accessed by MECS. Unauthorized access to a Google Domain account by any student is prohibited. All communication between students and staff must be through the MECS email address.

Students must refrain from using MECS email with the purpose of:
- Sharing their Google account access information (logins and passwords) with other students.
- Soliciting or using the account access information of others. Students shall be held personally responsible for all content in their Google Domain accounts stored in Gmail, Docs, Drive, etc.
- Downloading any file attached to an electronic message unless the student is certain of that message authenticity and the nature of the file,
- Sending personal and confidential information.
- Swearing, using vulgarities, or using any other inappropriate language in any email transmission (Disciplinary action, as outlined in this policy, may be imposed).
- Sending or forwarding chain letters.
- Spamming (sending unwanted, unsolicited emails to large groups of people, or everyone in your address book).

- Sending or sharing documents with large groups of people for anything other than an educational purpose to include selling products or offering outside merchandise.
- Subscribing to mail or notification lists (e.g. signing up or creating accounts for anything not school related).
- Sending emails with false or defamatory information.
- Sending emails that are intended to harass, insult, or are personal or discriminatory attacks on another user
- Confronting complaining, or sarcastic commenting while using email. Remember, people can't hear the tone of your words accurately while reading an email.

When communicating with MECS staff through Gmail, students shall use the MECS staff member's official email address. YouTube is offered to students through the Google Domain. A limited number of videos appropriate for school use are available in a restricted mode. Videos that are not available but have an educational purpose may be approved through MECS teachers and staff.

Violations of the expectations may result in the following consequences:
1. Discussion about an incident with student(s) involved.
2. Adjustment to computer privileges.
3. Changing filtering options to be more restrictive.
4. If any violation results in damage to a device provided by the school or of a device not their own, the device deductible is waived and the family is responsible to pay full replacement value for the damaged items.
5. Detention, suspension, and/or legal actions depending on the severity of the infraction(s).

Safety Measures and Limitations
As new technologies emerge, the educational value and ease of classroom integration will be evaluated concurrently by the MECS Technology Staff, Academic Director, Curriculum Coordinators, Spiritual Coordinator, and any other collaborator that could contribute to the process.

Data Backup and Network Security
Users shall not expect any data stored on MECS' computer system to be private. Digital communication and files stored on MECS' computer system are regarded as the property of the school. Authorized administrators may, without reason or prior notice, review files and documents including, but not limited to, email, documents, and logs, to ensure users are acting in accordance with this TAUP, and to maintain system integrity.
Current security measures include firewalls, Internet filters, virus protection, and virus monitoring devices.

Social Media
Social media includes Internet-based applications and mobile technologies that allow the creation and exchange of user-generated content. Examples of commonly used social media tools include, but are not limited to: blogs, message boards, chat groups, instant messaging, personal news updates, and music/video sharing (e.g., Facebook, Instagram, YouTube, and Twitter).

Students may use social media on MECS' computer system only for educational purposes, with prior approval from the classroom teacher.

Students should only interact with staff through social media sites created for educational purposes. Students should not engage staff through personal social media sites.