American School of Guatemala's Acceptable Use Policy for Technology—Students

Section 1. **Purpose of Technology Use**

The American School of Guatemala provides technology resources to its students solely for educational purposes. Through technology, the School provides access for students and teachers to resources from around the world. Expanding technologies take students and teachers beyond the confines of the classroom, and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence in the School for elementary, middle and high school by facilitating resource sharing, innovation, and communication with the support and supervision of teachers, support staff and parents.

The School committed to creating a safe and caring learning environment. We have designed a curriculum that includes safety and security, manners and values, bullying and ethics, research and information fluency. Through this curriculum we encourage the development of a personally responsible, collaborative community. Our values program supports and reinforces all these aspects.

Section 2. **The Opportunities and Risks of Technology Use**

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting, or that may be harmful or disruptive. Because information on networks is transitory and diverse, the School cannot completely predict or control what users may or may not locate. The American School of Guatemala believes that the educational value

of limited access to the information, interaction, and research capabilities that technology offers outweighs the possibility that users may obtain or encounter material that is not consistent with the educational goals of the School.

The School installs and operates filtering software to limit users' internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the educational process, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the School cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software, as explained in this agreement does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such inappropriate materials.

No technology is guaranteed to be error-free or totally dependable, nor is it safe when used irresponsibly. Among other matters, the School is not liable or responsible for:
- Any information that may be lost, damaged, or unavailable due to technical, or other, difficulties;
- The accuracy or suitability of any information that is retrieved through technology;
- Breaches of confidentiality;
- Defamatory material; or
- The consequences that may come from failure to follow these policies and procedures governing the use of technology.

Section 3. **Privileges and Responsibilities**

The School's electronic network is part of the curriculum and is not a public forum for general use. Student users may access technology for only educational purposes. The actions of student users accessing networks through CAG network reflect on the School; therefore, student users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Students are responsible for their behavior and communications using their computers and the CAG network.

Student users of technology shall:
- Use or access technology only for educational purposes.
- Comply with copyright laws and software licensing agreements.
- Understand that email and network files are not private. Network administrators may review files and communications to maintain system integrity and monitor responsible student use.

- Respect the privacy rights of others.
- Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.
- Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
- Abide by the policies and procedures of networks and systems linked by technology.
- Use *The Golden Rule* ("Don't do anything to others you wouldn't want them to do to you"). Be a good cybercitizen by respecting all others while using CAG electronic resources.
- Must cooperate with the installation of certificates or any other new measures deemed necessary by the Technology Department.
- Set the default search to Google as it is the main search engine used while on the CAG campus. Other browsers such as Safari, Mozilla Firefox, or Microsoft Edge are allowed, but default must be Google Chrome.
- Follow the same rules of conduct established in the CAG Family Handbook. Students are expected to use the same common sense on CAG electronic resources as they would in any other area or activity.

Students may not use the technology for improper uses. These uses include, but are not limited to:
- Any and all illegal purposes;
- Any and all obscene or pornographic purposes, including, but not limited to, retrieving or viewing sexually explicit material;
- Any and all discriminatory purposes, including harassment and bullying of individuals based on race, gender, religion, sexual orientation, or disability, among others;
- Any use of profanity, obscenity, or language that is offensive or threatening;
- Reposting or forwarding personal communications without the author's prior consent;
- Reposting or forwarding of junk mail, chain letters, or inappropriate or offensive jokes;
- Destruction, alteration, disfigurement or unauthorized access of hardware, software, or firmware;
- Obtaining financial gain or Transacting any business or commercial activities;
- Plagiarizing (claiming another person's writings as your own);
- Political advocacy;
- Disrupting the use of others to any process, program or tool, including downloading or otherwise spreading computer viruses or malware;

- Engaging in hacking of any kind, including, but not limited to, the illegal or unauthorized access;
- Allowing others to use Property issued without authorization, including students whose access privileges have been suspended or revoked;
- Soliciting or distributing information with the intent to incite violence, cause personal harm, damage a person's character, or to harass another individual.
  Any and all other purposes that would violate the Student Code of Conduct.

INTERNET SAFETY:

Students must take steps to ensure their safety on the internet, including, but not limited to, the following rules:

- Students should not share their private information or that of other people online. Private information includes: name, address, phone number, name of the school, activities which reveal schedules and/or locations.
- Students should not provide their full name or other contact information at any time.
- High School students do not have to provide personal contact information unless required by another school for educational purposes, including admission to universities, jobs or activities of academic and professional development.
- Students should not agree to meet in person with someone they have met in cyberspace.
- Students must notify a school leader, teacher or school employee regarding any message they receive that is inappropriate or makes them feel uncomfortable.

Email

CAG provides email service to be used for projects/educational activities and all communication within the school community. The email account is not intended to be used for event invitations or fundraising purposes. Responsible digital citizenship is expected at all times while using this account. Mass emails must be approved in advance.

Expectations for Use

- Personal email accounts can be accessed through the school network for educational purposes only (access or sending documents related to educational activities such as tasks, projects or links).
- Users must avoid signing for a third party or impersonating someone else.
- All teachers and students must use their CAG email account for all school activities and check it frequently.
- Users must avoid forwarding private messages without the original author's consent or emails that contain private information about another person.
- Users can send messages to a maximum of 20 recipients at a time. Each shared group counts as one recipient.

- When a student is no longer a member of the school community, their account will be closed and deleted from the system within one month after their last day. They should report a personal email address to contact them in the future.
- Students must share their username and password with their parents.
- Every community member needs to sign the agreement form when their account is created/activated and comply with the established email address format. For students, the following format is used:
username: ID number
password: same password used to log into the network account.

Social Media

If you participate in social media on behalf of CAG, the School expects you to follow these basic principles:

- Engage in social media with a clear plan, strategy, goals, and line of responsibility. That means being responsible for continuous monitoring, maintenance, and timely responses.
- Add value with unique, strategic information and commentary about CAG.
- Be transparent, and avoid misrepresentation.
- Write about what you know, and stick to your area of expertise when commenting.
- Always pause and think before posting, and consult with a teacher or expert if unsure.
- Post meaningful, respectful comments — no spam or off-topic or unprofessional remarks. If you make a mistake, admit it — and be upfront and quick with your correction.
- Handle negative comments and developments quickly, professionally, and strategically.
- Respect confidentiality of all participants, and never disclose student information.
- Give credit to sources of written content, images, and ideas, you reference or use.
- Always use proper grammar and write clearly.
- Know and follow CAG policies on behavior, social media age limits, values and technology.

Websites and Web Pages (applies for social media pages such as Youtube, Facebook, Instagram, Snapchat, LinkedIn, Twitter, etc.)

- Students are allowed to publish respectable photographs and students can be identified by their full name with prior parental approval. Using the first name and initial of the last name can be used to identify photographs of groups or individuals. Parents may choose not to authorize the identification of their children.
- The material published on the Internet must meet academic expectations with regard to spelling, grammar and accuracy of the information and include references or citations.
- The material (graphics, sounds, text, etc.) belonging to another person may not be published without proper authorization from the author. The authorization note must be included.

- All classroom pages should have a link created to Google sites through the school website or the class.

Section 4. **Security System**

The School has a virtual security system that is configured to block spam and sites that are not suitable for educational purposes. The administrators will monitor sites and determine if any additional sites should be blocked once identified. In addition, only the Technology Department is allowed to install software or download executable files.

- Students are held responsible for their personal accounts and must take all reasonable precautions to prevent others from gaining access to their accounts.
- Students must report any identified security problems with their accounts.
- Students should not attempt to gain unauthorized access to any of the School's electronic resources, destroy database systems or intentionally spread viruses.
- Files stored on the School's network are routinely maintained and monitored, which means no files are completely private and secure from the senior administration of the School.

Section 5. **Personal Devices (BYOD)**

Technology is required to enhance the learning experiences. Using appropriate technology makes the students get involved deeper in the learning. It also develops higher order thinking skills, technological fluency and they become better prepared to participate in tomorrow's world.

- Elementary (Grades 4-5) students are recommended (but not required) to have iPad or laptops that meet the minimum specs below.
- Middle and High School (Grades 6-12) students can bring any laptop that meets the minimum specs below. iPads, Microsoft Surface, and Android devices do not meet the minimum requirements for a primary device. However, students may bring one of these tablets as a secondary device to their main laptop. CAG recommends iPad or Surface over Android because Android devices may not be compatible with the CAG Network security.
- CAG recognizes that cellphones/mobile devices are powerful learning and communication tools. Cellphone use will be allowed in the classroom at teacher discretion.

Minimum Specifications

The following chart should help you in selecting and purchasing a laptop for your child to use while they are at The American School of Guatemala. While there are many options, there are minimum specifications that we require to support your child's learning at CAG.

Machine Type	Laptop
Platform	PC/Mac
Screen Size	11 inches or more
Processor	Intel i5 or Higher AMD Athlon II or Higher
RAM	6 GB or Higher
Hard Drive	500 GB or Higher
Operating System	Windows 10 or Higher, MacOS El Capitan, Sierra, or High Sierra
Wireless	802.11n or Higher
Ports	2 USB ports, Audio in/out, Built-in microphone, VGA or HDMI
Battery Life	4+ hours (4+ cell or higher)
Warranty	3 Year warranty with Damage protection

Students are expected to:
- Be completely responsible for his/her device and any extra equipment that accompanies the device;
- Label all devices with their name and CAG ID Code;
- Bring all devices fully charged;
- Password protect their devices;
- Have the locator activated;
- Comply with the regulations stipulated in the agreement.

Section 6. **Limitation of Liability**

The American School of Guatemala is not responsible for any lost, damage to devices, damaged caused viruses, or any data loss caused by interruption of services. In addition, the School is not responsible for the accuracy of quality of information obtained or stored in CAG's electronic resources.

Parents are highly recommended to do the following:

- Purchasing Damage Protection for your devices;

- Request you to include the device on your personal or home insurance. The laptop should be insured for accidental damage and loss by fire and theft when outside the home. The insurance can be purchased with your computer vendor or any insurance company. All insurance claims must be settled between parent and the insurance company.

Section 7. **Disciplinary Actions**

Violations of this policy, or any administrative regulations and guidelines governing the use of technology, may result in disciplinary action which could include loss of network access, loss of technology use, suspension or expulsion, or other appropriate disciplinary action or legal action. Additional disciplinary action may include other consequences, such as:

- Use CAG electronic resources only under strict supervision
- Restrict the use of electronic personal devices on campus
- Suspension of privileges on the network, use of equipment or school
- Conditioned re-enrollment for the following year
- Legal action by the authorities

Administrators will determine the consequences for breaches of this policy.

Your acknowledgment through the enrollment/re-enrollment process implies and that you and your child(ren) have read and agree to follow the Acceptable Use Policy of the American School of Guatemala.

Document Control
Preparation

Action	Name	Date
Updated to Repository	*Marvin García Castellanos*	*Apr 09, 2018*

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
1.0	July 1, 2012			Creation
2.0	July 1, 2016			Revision
3.0	July 1, 2017		4, 5, 7-10	Updated
4.0	April 09, 2018		All	Updated

Control and Revision
This document and its enclosing procedures and/or policies must be revised and updated at the most, 365 days after the latest release date.