



# Hill Country

## CHRISTIAN SCHOOL *of Austin*

### Acceptable Use of Technology

*Guided by God-honoring principles, Hill Country Christian School of Austin utilizes technology to inspire learning, expand resources, generate ideas, improve communication, facilitate collaboration, and transcend the walls of the classroom.*

Hill Country Christian School of Austin acknowledges that technology is an important tool in expanding learning opportunities and conducting scholarly research and is therefore committed to the integration of technology in the instructional process. To this end, Hill Country provides network access for students, faculty, support staff, and administration. Our goal is to promote educational excellence by facilitating research, sharing resources, enhancing communication, fostering collaboration, and encouraging innovation. All network access is expected to support educational research and to be consistent with the mission and educational goals of Hill Country Christian School. The use of the network is a **privilege**, not a right, and **inappropriate use will result in disciplinary action**.

This *Responsible Use Policy* is designed to give students and their families clear guidelines regarding the appropriate use of technology while using their own devices on campus or while using any school owned or issued computer or mobile device.

#### **Network Access:**

- All students in grades 7-12 are provided unique log in credentials. The User name may not be changed in any part under any circumstances. Students are initially provided a default password that must be changed at first login. Students must provide the new password to the Technology teacher, Technology Integration Specialist, or Librarian.
- Students are not to share their password with any other student.
- Students must provide their password to faculty/administration upon request.
- Students are responsible for any activity that occurs on school owned computers and devices while they are logged in.

- Students must log off of any computer when leaving it unattended. Students may not use the school network for personal or business reasons.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal law. This includes tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.
- Students must not make any attempt to access servers or network information that is not open to the public.

### **Computer Labs:**

- Students are encouraged to use the computers in the library, upper, and lower school labs for research, work completion, and projects when use would not interfere with classes in those locations.
- Students should make no changes to the appearance of the desktop or screensaver without express permission from the faculty member in charge.
- Students may not download or install any software, games, music, videos, or other applications on desktop or lab computers.
- Students may use only their own log in information to access school computers. Log in information should not be shared with other students.
- Students are responsible for any activity that occurs on a school computer under their log in credentials.
- Computers in the labs operate on the secure Student Network. Students must not make any attempt to access servers or network information that is not open to the public.

### **Personal Laptop Computers or Mobile Devices:**

- Students may not use their personal laptop computers or mobile devices at any time on campus during the school day unless taking part in specific in-class activities directed by the course instructor.
- Students using their personal laptops as part of a specific in-class activity are accountable to the same guidelines as students using school owned devices with regard to networks, the Internet, and content acceptability.
- Students using personal computers or mobile devices while on campus will not be able to access the secure school networks. All Internet access will be through the open wireless service belonging to Hill Country Bible Church Northwest.
- Students found to be in violation of this *Acceptable Use Policy* while on a personal computer or mobile device on campus will be subject to disciplinary action.
- Hill Country Christian School of Austin is not responsible for any loss, theft, or damage, both physical and data, to personal student computers or mobile devices.

**Internet Use:**

- The Internet is a rich and valuable source of information for education. Inappropriate materials are available on the Internet and are strictly prohibited. These materials include, but are not limited to, items of a sexual or pornographic nature, anti-religious, extremist, or militant materials, gambling, depictions of violence, and images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.
- If a student accidentally accesses a website that contains obscene or pornographic or otherwise offensive material, he or she is to notify the teacher or Technology Integration Specialist immediately. This is not merely a request, but a responsibility of all Internet users.

**Copyright:**

- Information obtained through the Internet must be properly cited and in compliance with all copyright laws. Due to the quickly changing nature of the Internet, a hard copy of referenced material is recommended.
- Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music and text.
- Plagiarism includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet sources will be treated the same as any other incidence of plagiarism.
- Lectures, notes, and other study aides created by faculty are the intellectual property of the faculty member, and as such are not to be used without permission of the faculty member and correct citation of the work.
- Unauthorized duplication, installation, alteration, or destruction of data, programs, hardware or software is prohibited.

**Privacy and Safety:**

- Students may not give any personal information regarding themselves or others through e-mail or the Internet, including name, phone number, address, passwords, etc., unless they are absolutely sure of the identity of the person with whom they are communicating. Frequently, the identity of someone on the Internet is impossible to confirm; therefore, contact with such individuals is considered inappropriate and unsafe.
- Students are not to provide the e-mail address or other personal information regarding other students, faculty, or administration to anyone outside of the school without their permission.
- Hill Country Christian School respects the privacy of every student, faculty member, and administrator with respect to stored files and e-mail accounts. However, if inappropriate activity, including harassment and bullying, is suspected, school officials reserve the right to view these files in order to investigate suspected inappropriate behavior or content.

- Hill Country Christian School reserves the right to monitor computer activities that take place, including blogging, website access, e-mail, bandwidth, and network use.



# Hill Country

CHRISTIAN SCHOOL *of Austin*

## Acknowledgement of Acceptable Use Policy 7<sup>th</sup>-12<sup>th</sup> Grade Students and Parents

### **Student Section:**

Student Name: \_\_\_\_\_ Grade: \_\_\_\_\_

By signing below I acknowledge that I have received a copy of and understand the Acceptable Use of Technology Policy of Hill Country Christian School of Austin. I understand that my activities on school owned and personal computer and mobile devices is subject to the guidelines laid down. I understand that my activities may be monitored by school officials. I understand that violation of this policy will result in disciplinary action and possible legal consequences.

I understand that the use of the technology resources provided by Hill Country Christian School of Austin is a privilege. I agree to abide by this policy.

Student Signature: \_\_\_\_\_ Date: \_\_\_\_\_

### **Parent or Guardian:**

I understand the Acceptable Use of Technology Policy and that all computer activity is not private. In consideration of the privilege accorded my child of using the Hill Country Christian School of Austin technology resources, I hereby release the school, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including without limitation, the type of damages identified in the school policy.

Parent/Guardian Printed Name: \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_



# Hill Country

## CHRISTIAN SCHOOL *of Austin*

### **School Issued Mobile Devices:**

- Students who are issued a school owned mobile device may make no attempt to circumvent the safeguards in place to monitor activity on the device. This includes, but is not limited to, the installation of alternate web browsers and “jail breaking” the device to remove it from the network.
- Students are required to download and maintain the appropriate applications on the device as directed by course instructors. These “apps” should be considered in the same vein as a textbook or school supply. They are necessary for the completion of the coursework.
- Students are allowed to load personal apps and music to the mobile device, but they are responsible for the content and nature of the items installed. Inappropriate material is subject to removal and disciplinary action where deemed appropriate.
- Students must surrender their device upon request by teachers or administrators at any time for maintenance, spot checks, and when monitoring software reports possible suspect activity.
- Web browsing on the mobile devices is being monitored both on and off campus. Students will be held accountable for any activity on the device at all times.
- Students are required to carry and store their devices in the cover provided.
- Coaches, teachers, and any other adult conducting a before or after school activity must provide a secure area for the devices during the activity.
- Students may not have inappropriate screensavers or backgrounds.
- Devices must not be left unattended at any time. Devices found unattended will be turned in to the Technology Integration Specialist or Technology Teacher and may be retrieved between classes, during lunch, or at the end of the day. Consequences may increase with repeated offenses.
- Devices must be in a student’s possession or secured in a locked classroom or locker at all times.
- Mobile devices are not allowed in the lunchroom.
- Mobile devices may not be used in the restrooms.
- Devices should not be left visible in vehicles.
- Markings, skins, stickers, or anything that defaces the devices are not allowed.

- Removal of school placed ID stickers is strictly prohibited.
- Teachers may enforce consequences when a student does not have the mobile device in class.
- Chatting, messaging, Facetime, Facebook, Twitter, and other social media during the school day are strictly prohibited unless authorized or directed by faculty/administration.

**E-Mail:**

- Students may make no change to any part of the e-mail address under any circumstances.
- Using e-mail during class is prohibited unless authorized by faculty or administration.
- Students should always use appropriate language in their e-mail.
- E-mail services provided by the school are to be used only for the exchange of appropriate information.
- No inappropriate language is allowed, including derogatory, obscene, harassing or bullying messages.
- E-mail messages of an abusive, harassing, or bullying nature will be regarded as a violation of school rules and will be subject to appropriate disciplinary action.
- Chain letters of any kind and spam are prohibited. Spam is defined as any e-mail message asking you to pass information or messages on to other individuals or groups via e-mail.
- Students are prohibited from accessing anyone else's e-mail account.
- E-mail is subject to monitoring and auditing at any time with or without student knowledge or consent.

**Insurance:**

- An insurance policy covering loss, theft, accidental damage, and water damage is in effect for each mobile device checked out to students
- Students should immediately notify the Technology Integration Specialist if any of the above incidences occur. In the case of theft, a police report should be filed.
- Students are responsible for the \$100 deductible to cover the repair or replacement of the device.
- A loaner device will be issued during the time the student's device is out of service.