Technology Acceptable Use Policy

Introduction

Shiloh Christian School recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st Century technology and communication skills. To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that students are expected to follow when using technologies in school or when using their tablet computer or other electronic device on the SCS campus.

- The Shiloh Christian School wireless network is intended for educational purposes.
- All activity over the network or using school technologies will be monitored and retained.
- Access to online content via the network is restricted in accordance with our policies and federal regulations, such as the Children’s Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources may result in disciplinary action.
- Shiloh Christian School makes a reasonable effort to ensure student’s safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the SCS network or other technologies are expected to alert school faculty or administration immediately of any concerns for safety or security.

Using Your Tablet or other Electronic Device at School

Electronic tablets and other electronic devices (excluding cell phones) are intended for use at school each day. In addition to teacher expectations for the use of these devices, school messages, announcements, planners, calendars and schedules may be accessed using these devices.

Hot Spots and 3G/4G

Students are not permitted to connect to the internet using a detected hot spot or 3G or 4G account while at school. The IT department will be able to detect this on the school’s network.

Charging Your Device’s Battery

Tablets or other devices must be brought to school each day in a fully charged condition. Keep in mind that, currently, an iPad, for example, can take up to 5 hours to charge fully.

Screensavers/Background photos

Users of tablets and electronic devices are expected to choose appropriate wallpapers, screensavers, desktop, backgrounds, and/or displays for their devices which are consistent with school's core values and mission.

Photos

All technologies provided by or used at Shiloh Christian School are intended for education purposes. Students are expected to follow the Biblical mandate to honor the Lord Jesus Christ in all that they do. Therefore, students are expected to use technology is ways that are appropriate, safe, and cautious. Students are expected not to attempt to circumvent technological protocol measures. Further, students are expected to ask appropriate school personnel, should questions arise regarding matters pertaining to the use of these devices and their environments.

Sound, Music

On *school-owned tablets and devices* students may not download music from iTunes or any other music sharing site unless directed by or with the permission of a teacher. *On all school-owned devices*, sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

Gaming

Students may only use appropriate gaming apps during discretionary time and with approval. Discretionary time would not include classroom instructional time, chapel and/or other events or environments where use of devices would not be appropriate. School administration faculty, staff and/or sponsors always reserve the right to ask students to close their gaming app or to do random checks during non-discretionary time.

Saving Work

It is the student's responsibility to ensure that work is not lost due to equipment failure, failure to back-up files or deletion. Device malfunctions are not an acceptable excuse for not submitting work. Students should back up all work for their own protection.

Network Connectivity

SCS makes no guarantee that the school wireless network will be up and running 100% of the time.

Downloading Apps

Teachers may require students to download apps or electronic books that have application to their specific course content.

Inspection

Students may be required to provide their technology for inspection at any time.

Web Access

Shiloh Christian School provides students with access to the Internet and its content. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing will be monitored and web activity records may be retained.

Users are expected to respect that the web filters used are safety precautions and are not to be circumvented. If a user believes a site or content should not be blocked, the user should alert a member of school faculty or administration. Parents are encouraged to use the Settings function on devices to limit or disable specific inappropriate options for the environment of their intended use.

Email

Shiloh Christian School may provide users with a Gmail account for the purpose of school-related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown origin and should only communicate with other people as allowed by SCS policy or their teacher.

Users are expected to exercise appropriate, safe, mindful, and courteous communication. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, Shiloh Christian School may provide users with access to web sites, content and/or tools that allow collaboration, sharing, and messaging among users.

Posts, chats, sharing, and messaging may be monitored. Users are cautioned not to share personally-identifying information online. (see Social Media Policy)

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or distrusted origin.

If a user believes a device being used might be infected with a virus they should alert personnel in the school's IT department. A device user should not attempt to remove the virus using any means or methods.

Plagiarism

Users should not use content without appropriate citation. This includes usage of words and from the Internet or elsewhere. A misrepresentation of appropriate credit to the content's creator is considered plagiarism. All research should be appropriately cited. (See Plagiarism Policy)

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If a user should encounter any message, comment, image, or other content else online that causes concern for one's personal safety, it should immediately be brought to the attention of an appropriate adult.

Cyber-bullying

Harassing, denigrating, impersonating, pranking, excluding, and cyber-stalking are all examples of cyber-bullying. Cyber-bullying will not be tolerated. Sending emails or posting comments, images, and/or other content with the intent of scaring, hurting, or intimidating someone else can be considered cyber-bullying.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, can be a crime. These behaviors may also result in severe disciplinary action and loss of privileges. Remember network activities are monitored and retained. (See Anti-Bullying/Harassment Policy)

Parent/Guardian Responsibilities

It is strongly suggested that parents communicate with students about values and the standards they should follow regarding the use of the Internet and all media information sources such as television, cell phones, electronic devices, videos, movies, and music.

Examples of Acceptable Use

I will:

- Never leave my device unattended and I will know where it is at all times
- I will place some form of name identification on the case or device itself
- Use school technologies for school-related activities
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline
- Treat school resources carefully, and alert staff if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online
- Use school technologies at appropriate times, in approved places, for educational pursuits
- Cite sources when using online sites and resources for research
- Recognize that use of school technologies is a privilege and treat it as such
- Be cautious to protect the safety of myself and others
- Help to protect the security of school resources
- Recognize my network activities are monitored by school personnel

This is not intended to be an exhaustive list. Users should use their own good judgment when using technologies related to the school.

Examples of UN-acceptable Use:

- Spamming-Sending mass or inappropriate emails
- Gaining access to other student’s accounts, files, and/or data
- Use of the school’s internet/E-mail accounts for financial or commercial gain or for any illegal activity
- Participation in credit card fraud, electronic forgery or other forms of illegal behavior
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients
- Bypassing the SCS web filter through a web proxy, 3G, 4G or Hotspot
- Using another student’s device without permission of that student and a faculty member
- Illegal installation or transmission of copyrighted materials
- Any action that violates existing School policy or public law

- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials
- Use of chat rooms, sites selling term papers, book reports and other forms of student work
- Gaming during inappropriate times and/or using in appropriate games which contradict the school's core values and mission
- Attempt to find inappropriate images or content
- Engaging in cyber-bullying, harassment, sending sexually explicit photos, arranging to meet someone on-line or disrespectful conduct toward others
- Try to find ways to circumvent the school's safety measures and filtering tools
- Agree to a physical face to face meeting of someone met online
- Use school technologies for illegal activities or to pursue information on such activities
- Attempt to hack or access sites, servers, or content that isn't intended for my use

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies

Limitation of Liability

Shiloh Christian School will not be responsible for damage, harm or theft to student-owned tablets or other electronic devices. While Shiloh Christian School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Shiloh Christian School will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this acceptable Use Policy may have disciplinary repercussions, including but not limited to:

- Suspension of network, technology, or computer privileges
- Loss of device use for a determined period of time (student still responsible for all required work)
- Notification of parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution