Flint Hills Christian School

Acceptable Use Policy

(This material was taken from the Acceptable Use policies of the entities listed in the appendix.)

Note: These guidelines were formulated after careful review of school computer use and cell phone policies across the State and the country. (Christian Law Association, 2006)

Preamble

A good Acceptable Use Policy serves to keep students safe while allowing them to utilize the many technology and online resources now available to enhance or complement classroom learning. We want students to be critical consumers of information and learn that there are right and wrong ways to respond to various online situations.

In the past, an acceptable use policy's purpose was to protect school districts from liability resulting from inappropriate use. Many "acceptable use" policies listed what was unacceptable, and then banned it. That approach was somewhat effective when technology access was not so widespread as it is today. Now there is a definite need to shift from banning inappropriate use to modeling appropriate and responsible use. While some filtering and monitoring is necessary to maintain our network and protect students, it is not our goal to simply "catch" students doing something wrong or restrict their access information and textbooks provided by the online world. Filtering software is not 100% effective. Our goal is to teach and model good online behavior, ethics and skills, while still lowering risk to students and protecting the school from liability.

An online and Internet world is here to stay in modern life. The time to learn online and Internet safety is while also learning to use it in the educational and home setting. Use, knowledge and responsibility go together. We wouldn't put our students behind the wheel of a car without learning the mechanics of driving as well as the rules of the road, respect for the power of the vehicle and guidance for the choices that a student who is alone in a car may encounter. The Internet is no different.

Flint Hills Christian School aims to teach our students how to be responsible 21st century learners. They should leave FHCS bound for college and careers with skills that enable them to know how to use the Internet and online resources for the educational, research and communication purposes now expected of students by universities and employers. Students should learn technology skills in an environment that matches our existing school policies for behavior and ethics. Once they properly learn to use the tools, they will be equipped for life beyond our community with skills that will help them maintain the Christian values we instill while being knowledgeable about the digital world and how to safely navigate it. Our goal is to instruct them on how to manage any issues that will come up at school or beyond when they encounter a "bad" site, how to make good choices, evaluate the information they read and post, and how to self-moderate both time use and content access.

Access means that students will inevitably make mistakes. Most mistakes are just that, mistakes, and may simply require a quick discussion. Our mission includes correcting and guiding students in a manner appropriate for the age, infraction and pattern of abuse. Many times, this is all that is needed so students feel safe informing us of their actions when something becomes uncomfortable. They can learn the right and wrong of a situation and how to deal with it.

No Acceptable Use Policy is perfect or complete, but it gives students a framework with which to start and safely grow and learn. Our intent is to graduate skilled and informed digital citizens of integrity.

<u>Conclusion</u>

Our policies and uses of technology must be collaborative, conversational, and transparent as we grow in understanding of who we are together.

FHCS should model and teach students (and parents) appropriate online and digital behavior and hold conversations as needed between students, teachers, administrators and parents to form, explain, enforce and modify policy as needed.

Flint Hills Christian School Technology Use Policy

The Apostle Paul provides a good perspective in 1 Cor. 10 that can be applied to use of technology: "All things are lawful, but not all things are helpful. All things are lawful, but not all things build up." I Cor. 10:23. First, though there are many appropriate uses for technology, not all are appropriate or helpful during school hours. There are also other legal but inappropriate uses for technology contrary to our standards and policies as a Christian school. Above all, our desire is in keeping with Paul's: "So whether you eat or drink or whatever you do (including the use of technology), do all to the glory of God."

Due to the ever-changing nature of technology, it is imperative for everyone to realize that our policies regarding the use of technology in our community will also change as the need arises. We ask all students, employees, and family to utilize their best judgment when it comes to the use of school technology and keep in mind that our policies related to technology are not meant to supersede our other school policies, but rather to complement them.

All technology provided by the school is intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of its intent:

- Be Smart, Alert, Strong, Kind, and Brave [Google "Be Internet Awesome" Digital Citizenship Curriculum]
- Don't try to get around security and protection measures.
- Use common sense.
- Ask if you don't know.

Definitions

AUP	Acceptable Use Policy (in its abridged form here)
CIPA	Children's Internet Protection Act
FHCS	Flint Hills Christian School
Network	All devices and technologies (including computers, router, software, internet, etc.) used to provide technology services to the students and staff at Flint Hills Christian School
Device	Any computer, tablet, cell (or smart) phone or watch, or other such device used for the purpose of accessing the network at FHCS
Educational	Use of school provided technology to enhance classroom learning, promote independent research, provide for school administration, and prepare individual and collaborative assignments
PCD	Personal Computing Device (laptop, phone, tablet, e-reader, etc.)
Student	For the purpose of technology use, a student is defined as any administration approved K-12 individual on campus or using school technology off site, whether a currently enrolled FHCS student or guest.
System Administrator	Mr. Merv Bitikofer or his designee
School Administrator	Mr. Joshua Snyder

Policy

Our school's technology infrastructure exists to support our educational mission. To that end, it is provided for use by students and staff. This Technology Use Policy outlines the guidelines and behaviors that students are expected to follow when using school technology or when using personally owned devices at school.

Technology as a Privilege

The use of technology resources on school property or at school events is a privilege, not an entitlement. This privilege comes with personal responsibilities and if you violate the responsible use of any school technologies, your privilege may be revoked and/or suspended. FHCS reserves the right to limit your access. Access entails responsibility.

Responsibilities

As a user at FHCS you may have access to school Electronic Resources (network, email, voicemail, telephones, computers, tablets, facsimile machines), including the network and Internet. The network is viewed as an extension of the FHCS community and all expectations regarding standards of behavior as outlined in the Student Handbook apply to your actions while utilizing or accessing the network or other Electronic Resources. We expect our students and staff to act responsibly and thoughtfully when it comes to using technology. Users bear the burden of responsibility to inquire with the technology coordinator or school administrator when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

Privacy

The FHCS network is a private network owned by Flint Hills Christian School. The network is maintained and managed by the system administrator as to ensure its availability and reliability in performing its educational mission. The school reserves the right to monitor all behaviors and interactions that take place online or using technology on our property or at our events for the protection of both students and the school. We also reserve the right to investigate any reports of inappropriate actions related to any technology used at school or online posts reflective of the school community. A teacher or administrator may review student files and communications to maintain system integrity and to ensure that users are using the system responsibly when deemed necessary by student behavior or if reasonable cause exists. FHCS may do so without prior notice to the user.

Students have a limited expectation of privacy when using their own technology on school property. The same rules and sanctions that apply to school-owned technology also applies to personally owned devices on the school property or at a school event.

Technology Covered

Flint Hills Christian School may provide internet access, desktop computers, laptops, Chromebooks, tablets and other mobile devices, email, and accounts with such educational technology providers such as Google, FACTS (Formerly RenWeb), Canvas, College Board, as well as other educational sites as they relate to classroom curriculum and assignments. This policy is intended to cover existing technology in use at FHCS as well as future technology that FHCS acquires and may provide.

Purposes and Use Expectations for Technology

The use of all school-owned technologies including the school Internet connection for students is limited to educational purposes. Educational purposes include, in part, classroom activities, career development, communication with experts, homework, and collaborative projects.

Students may not use any technology personal or school owned during school hours to play games, visit social networking websites, send instant messages or enter "chat" or "hangout" rooms without express permission from a teacher or administration.

Web Access

Flint Hills Christian School provides its users with access to the Internet, including websites, resources, content, online tools, and apps. Parent permission for access is required for minors. Access will be restricted in compliance with CIPA regulations and school policies.

Although FHCS has a content filter for Internet access, it is not 100% foolproof. The system administrator can audit all Internet access by FHCS users and web activity records may be retained indefinitely. No user should visit inappropriate sites. If this happens accidentally, the system administrator or teacher should be notified immediately.

Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the web. If a site is blocked and a user believes it shouldn't be, please inform the system administrator or a teacher.

School Owned Devices Policy

FHCS may provide users with desktop or mobile devices to promote learning both in and out of the classroom. Users are bound by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution. These are expensive devices that the school is entrusting to the user. Users should immediately report any loss, damage, or malfunction to the system administrator. Users may be financially responsible for any damage resulting from negligence or misuse.

The school reserves the right to monitor school-owned mobile devices off the school network.

Personally Owned Devices Policy

Students should keep personally owned devices (including but not limited to laptops, tablets, smart phones, cell phones, e-readers, etc.) turned off and put away during school hours unless granted permission by school personnel for educational purposes or in the event of an emergency. When personally owned devices are used on campus, they should be used over the secure, filtered wireless network. Before any student can log onto the school wireless network, their personal device must be registered with the system administrator. Under no circumstances should a student attempt to circumvent network policies or security.

Personal laptops and tablet devices, as well as school computers, may only be used for education purposes or teacher-authorized activities during the school day. Students may not play games, listen to

music, instant message, chat or otherwise use these devices during school time for non-educational purposes without express permission from a teacher or administrator.

Security

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

Users should alert the system administrator or his designee if they suspect that one of their devices is infected with a virus. Users should not attempt to remove the virus or download any programs to help remove the virus.

Keep backup copies of important work. Properly use the features for security or sharing access to your information on any device you use.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birth date, or financial information (i.e. credit card numbers, bank numbers, etc.) over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity with associated risks and should carefully safeguard the personal information of themselves and others. Users should not communicate with strangers over the Internet and should never agree to meet someone they met online in real life without parental permission.

If at any point, users see a message, content, image or anything else online that makes them uncomfortable or concerned for their personal safety, it should be brought to the attention of a teacher or administrator immediately.

Do not share your password(s) with anyone other than teachers, the school administrator, and parents as requested or required. Change your password periodically unless directed otherwise by a teacher or administrator. You are responsible for anything that happens on the school network that is associated with your login information. This applies to all school-related accounts such as using a desktop computer or accessing email, FACTS (formerly RenWeb), Canvas, or other school-related app or program.

Email

FHCS provides students 6th grade and above with email accounts for the purpose of school-related communication. This will be the account of record for all student school use, and should be used when communicating with teachers, coaches, and administrators. All existing handbook policies apply to the use of these accounts. The 6th grade class email accounts will be subject to special monitoring as they transition toward secondary status. FHCS student email accounts should not be used for mass emails that are not related to academic or FHCS extracurricular activities. It is permitted – even recommended – to use this account for collaborative assignments with classmates. In all use of this account, students are bound by ethical and moral considerations as outlined in the student handbook. Availability and use may be restricted based on school policies.

If students are provided with email accounts, they should be used with care. Recognize limitations to privacy in electronic communication. Email is not guaranteed to be private. Students should not send personal information, should not attempt to open files or follow links from unknown or untrusted origin, should use appropriate language, and should only communicate with other people as allowed by school policy. School administrators, teachers and parents may request to know student email passwords for use as necessary for educational or disciplinary purposes.

Students are expected to identify themselves clearly and accurately in electronic communication. Misrepresenting oneself or falsifying a name or using another's name is not allowed. Communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Google Apps/Canvas/Social Networking/Collaborative Content

Recognizing the benefits that collaboration brings to the learning environment, FHCS may provide users accounts with Google, Canvas, FACTS (formerly RenWeb), or other tools in order to facilitate collaboration between students, teachers, and other staff members. Use of these platforms and tools may be restricted based on school policies.

Users should ensure that any documents or collaborative projects are shared with others as allowed by school policy.

Content created and saved by students while using software or accounts owned by the school is considered the intellectual property of the school and may be retained for use by the school if the student leaves the school for any reason. Apps and programs purchased by the school are school property and stay with the device even if the user no longer uses or has access to the device.

Students of FHCS should also take care to be appropriate, safe, mindful, and courteous in their personal use of technology outside of the school. Posts, chats, messages and other forms of communication and networking should not poorly represent the school and its families outside of our building and all school rules for conduct should be followed, offline as well as online. Students are expected to abide by the school behavior policy on and off campus, in person and online. Students may be asked to remove posts deemed inappropriate or found to violate school policy.

Student Use of Cell Phones/Smart Phones/Smart Watches/AirPods

School policy on cell phone use is intended to accomplish the following:

- Minimize distraction and disruption to the school environment
- Promote face-to-face interaction and bonding
- Train students to use cell phones and their functions (photos, videos, texting, social media) in a way that maximizes their positive potential while mitigating negative consequences. That is: training students WHEN, WHERE, and HOW to use their devices.

The following policy attempts to balance these three goals, giving students freedom to use their devices at approved times to take photos, check social media, text parents and others etc. If abused, these freedoms may be restricted or revoked for individual students or the secondary school as discerned by the Administrator or his designee. Students with signed technology contracts and parental permission can use cell phones and personal devices while on campus in the following ways.

Students may have **free access** to cellphones and devices **before school, after school, and during morning break** if this usage does not violate other stated policy. This includes:

- Taking photos or videos
- Checking social media
- Texting
- Listening to music, watching videos, etc.

Cellphones are not to be accessed or used during passing periods.

Cellphones are not to be accessed or used during lunch. Since we at FHCS value face-to-face interaction and socialization, students should use lunch as a time to be present with their teachers and peers w/o digital devices. **Devices must be left stored in hallway lockers (not in backpacks or in locker rooms)** for the entirety of the lunch period until they return to the main building.

If a student wishes to access their device outside of these timeframes, they should seek out a teacher and ask permission. **As much as possible, parents should contact the office when needing to get an urgent message to their child.**

Teachers will have a container in their room where students will be required to deposit their phone upon entering the classroom. They may be picked up at the end of the class period.

Students are always expected to access the school's wireless network to connect to the Internet on their cell phones and approved personal devices. This means **no 3G, 4G, 5G, hot spots or tethering** for data access while at school. The FHCS wireless password will be entered by staff members on personal phones and devices at the beginning of the school year or at any time the password changes throughout the school year. The FHCS wireless password should not be given by administration, teachers or parents to students.

Devices used inappropriately may be confiscated by staff and turned in to the office. The student will have to see the principal to get the device back at the end of the day. The office will email or text the parent to let them know that their child's phone was taken. Bringing electronic devices on campus is a privilege and not a right. Consistent abuse of devices during school time may result in requiring the student to leave his/her device at home, in their car or at the school office during the school day. Repeat infractions will be considered rebellious and insubordinate behavior and be subject to the appropriate discipline as outlined in our handbook.

Students **can take photos and record videos at school at approved times** as long as they abide by all other school policies in nature of content and use. They are not to be used to embarrass, bully, or harass others and all media taken, shared, and posted must be with permission of all included. Any media taken on school property that violates school policy or raises concern may be asked to be deleted and consequences may follow. **Particularly, no cell phone use ESPECIALLY photographs/videos are permitted in the bathrooms or locker room areas (ex. during volleyball, basketball, etc.) at any time. Devices should be kept in hallway lockers or common areas and not stored in locker rooms.** Violation of this prohibition is a serious discipline offense.

Because modern cell phones may also function as data storage devices, student cell phones brought to school are subject to inspection and review by school staff when student behavior deems this necessary.

Any contraband content or content deemed to be inappropriate in the sole discretion of the administration may be grounds for further discipline.

The school will not be held responsible for any loss or damage to a student's cell phone or other devices while at school.

Online Behavior

Ethical behavior is expected of FHCS students in all situations. Students are expected to maintain a Christian ethic regarding the use of technology both on campus, off campus and online. Flint Hills Christian School recognizes a student's rights to freedom of speech, expression and association – this includes the use of online social networks. In the context of being a FHCS student, however, attending FHCS is a privilege, not a right. As a student, you represent FHCS and are expected to portray yourself, your family, and FHCS in a positive manner. Any online postings must therefore be consistent with the ideals and policies of FHCS, as well as Federal Laws.

A higher degree of anonymity exists with the Internet than is experienced in face-to-face communications. The anonymity tempts some to behave in antisocial ways, e.g., bullying, insulting, inappropriate pictures, posts, etc. Certain internet sites and mobile apps including, but not limited to Twitter, Instagram, YouTube, Snapchat, Reddit, Facebook and personal web pages, etc., offer easy communication and insight into many other people's lives, but can also contain slander and misinformation. Students are reminded that if they are posting on the internet (whatever the venue) they should do so with care and with the student handbook in mind. It is unacceptable for students to engage in cyberbullying, harassment or intimidation at any time, whether on or off the school's network. Students should also be aware that when posting to a personal account, even if marked 'private', it is possible that at some point it will be seen by people for who it was not intended. Posting is publishing, it leaves a digital footprint, and posts reflect on the character of the author. Students should also remember not to post anything online that they wouldn't want parents, teachers, or future employers to see. For example, a public post on a social media account in 9th grade may be seen by college scholarship committees, admission counselors or future employers many years later. Again, existing policies demand that FHCS students exhibit the highest moral and social behaviors; these references are only made here to reinforce those policies. Remember: screenshots and actual screen display video recording is easy to do on a cellphone or computer – just because you only shared it with friends does NOT mean it won't be seen or shared later without your permission or knowledge.

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research.

Cyber-Bullying

Cyber-bullying will not be permitted. Harassing others in any way is not allowed. Communication sent or content posted, from school or home, with the intent of scaring, hurting, embarrassing or intimidating someone else will not be tolerated. If users engage in such activity, they are subject to severe disciplinary action. Keep in mind that in some cases, cyber-bullying can be considered a crime.

Computer Settings and Computer Labs

Students are only allowed to alter, change, modify, repair or reconfigure settings on school-owned computers with the express prior permission of a teacher or the system administrator. This includes deleting cookies, bookmarks and history and resetting the time and/or date on the computer.

Downloads

Users should not attempt to download or run .exe (executable files) programs over the school network or onto school resources without express permission from the system administrator or another staff member.

Do not install software from home without permission.

Apps or other files should only be downloaded, with permission, from trusted, reputable sites and only for educational purposes.

Acceptable Use of School Technology

The use of all technology resources at Flint Hills Christian School should always be acceptable and pleasing to God. It is understood that Internet access for the student is a privilege, not a right. All users of the Internet will agree to adhere to the following code of ethics:

> *I will strive to act in all situations with honesty, integrity, and respect for the rights of others and to help others to behave in a similar fashion. I will make a conscious effort to be a good testimony to my fellow students, teachers, administrators, and others I communicate with on the Internet. I agree to follow Flint Hills Christian School's rules. I will strive to apply Philippians 4:8 to my electronic communications.*
>
> *Phil. 4:8 – "Finally brothers, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable – if anything is excellent or praiseworthy – think about such things."*

Users may make use of FHCS technology for purposes of education, academics, research, business operations, and school classroom related activities and/or communications. Students are expected to:

- Always know where their device is.
- Have some form of name identification on the case or device itself
- Follow the same guidelines for respectful, responsible behavior online that they are 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 threatening, inappropriate or harmful content (images, messages, posts) is seen online
- Use school technologies at appropriate times, in approved ways.
- Cite sources when using online sites and resources for research
- Be cautious to protect the safety of myself and others
- Help protect the security of school resources

Unacceptable Use of Technology

No policy can detail all possible examples of unacceptable behavior related to technology use. Some examples of unacceptable uses of technology are included below. This list is in no way meant to be exhaustive.

Unacceptable Use of Flint Hills Christian School Technology

- Involvement in any activity prohibited by law.
- Intentional use of invasive software such as viruses, worms, Trojan Horses and other malicious software.
- Interfering with the normal and proper operation of this network, the Internet or any other network. This includes hacking, cracking, probing, attempting to gain access to unauthorized accounts and equipment, utilizing excessive amounts of bandwidth, and attaching any type of hardware without express permission.
- Adversely affecting the ability of others to use equipment and services.
- Use of a camera or microphone in any school building or on campus is prohibited without direct permission by a staff member and all parties involved in the photo, video or recording.
- Tampering with computers, printers, network devices and other equipment belonging to FHCS or other people. This includes any attempt to alter, change, modify, repair or reconfigure computer and mouse settings without express prior permission from a teacher or system administrator. These settings include but are not limited to desktop images, mouse settings, moving or deleting icons and shortcuts on the desktop, changing default programs, navigator, screen display settings, installing any software not authorized by a teacher. It also includes adding extensions or internet plugins without teacher permission. Ex. Grammarly, AdBlocker
- Use of chat or hangout features, online messaging, or other social media apps such as Facebook, Twitter, Instagram, YouTube or Reddit without teacher permission. YouTube may be used under teacher supervision for educational purposes. Exceptions would be use of chat features in school provided programs that gives a safe, school monitored area for chatting and collaborative projects and communication w/permission.
- Downloading files w/o permission.
- Using the network for financial and/or personal gain or for political lobbying except as expressly allowed during a school activity.
- Attempting to logon to any computer, device or the network as the system administrator or gain access beyond your authorized access level. Ex. Asking for or sharing the school Wi-Fi password.
- Trespassing in another's folders, work or files or using another person's account.
- Changing computer files that do not belong to you.
- Utilize software or communication protocols not provided by FHCS or utilize any technology with the intent of bypassing or circumventing the FHCS security infrastructure.
- Add new or unauthorized devices such as hubs, switches, gateways, routers, access points and/or servers of any kind to existing FHCS technology.
- Using any "incognito" browsing window that makes user activity untraceable
- Possess, willingly receive, create, transfer or otherwise use any text, image, movie or sound recording that contains pornography, profanity, vulgarity, obscenity or language that offends or tends to degrade others.

- Sending or forwarding “chain” type letters, hate mail, anonymous or threatening messages.
- Viewing, storing or transferring obscene, sexually explicit or pornographic material.
- Use of recording equipment, whether audio, video, or both in school buildings or on school property without express prior permission from administration or a classroom teacher.
- Use of a camera, microphone or smartphone to record or take pictures of individuals which could be considered inappropriate, illicit, or sexual or embarrass anyone in any way. Use of these types of devices in the bathroom or locker room for any reason or to engage in personal attacks, harass another person or post private information of another person.
- Posting or sending email, SMS text, group chat or voicemail messages that are personal attacks, including any prejudicial, discriminatory, racist or sexist content, could cause damage or disruption, contain false or defamatory information about a person or organization, harassing another person. This includes attempts to bully or threaten as well as to incite violence or imminent threat of violence. If you are told by a person to stop sending them messages – you must stop. This also includes posting online gossip affecting the school community. This also includes group chat and communications that negatively affect student wellbeing or the environment of the school. Group chat should not be used for school related activities w/o teacher monitoring and supervision.
- Posting personal contact information about yourself or other people. This includes your address, telephone, school address, etc.
- Meeting with someone you have met online without the express approval of your parents or guardians and the Administrator.

Disciplinary Actions

Violation of this Technology Acceptable Use Policy is considered a violation of a school rule. Some behaviors are considered violations of a major school rule. Violations will result in one or more of the following disciplinary actions or consequences (FHCS will decide in its sole discretion which disciplinary action is warranted under the circumstances):

- Discussion and clarification about what happened.
- Verbal warning
- Written warning
- Notification of Parents
- Restriction of access privileges
- Removal from a class activity
- Removal from a course
- Confiscation of computer or other electronic equipment, including smartphones
- Student detention, restrictions or work hours (even if this interferes with an already scheduled school extracurricular activity)
- Suspension or expulsion
- Payment for damages due to your actions
- Referral to legal authorities

Other Expectations

Recognizing its responsibility to safeguard the name and reputation of our community, the Administration of Flint Hills Christian School reserves the right to respond as it sees fit to the

misbehavior of its students. The School Administrator may assign disciplinary consequences and/or counseling, even if the misbehavior takes place outside of school hours and away from school grounds or activities.

Limitation of Liability

While FHCS has systems in place to combat viruses, spyware, spam and other computer "bugs," FHCS will not be responsible for damage to a user's technology that results from viruses, spyware, malware, spam, or any other use of FHCS technology. Users are responsible for adequately protecting and maintaining their own technology.

Flint Hills Christian School will not be responsible for damage or harm to persons, file, data, or hardware. While FHCS employs filtering and other safety and security measures and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. FHCS will not be held responsible, financially or otherwise, for unauthorized use of its network or for transactions conducted over the school network. You are responsible for your activities.

Computer User Agreement for FHCS 6th through 12th Grade Students

Computer Lab and Network

I **will** use all technology items as tools to accomplish God's work in ways that please God.

I **will** use discernment in using computers to practice high standards of Christ-like living.

I **will** use the network and its programs for educational, school-related purposes only unless otherwise approved.

I **will** use the computers only with a teacher's permission.

I will use my school-issued email for school-related activities and will check it regularly.

I **understand** that passwords are private. I will not allow others to use my account name and password or try to use that of others.

I **will be** polite and use appropriate language in my email messages, multi-user role-playing and/or virtual learning environments (e.g. Google, Microsoft, Canvas), online postings, and other digital communications with others. I will refrain from using profanity, vulgarities, or any other inappropriate language as determined by school administrators on the network.

I will use email and other means of communications responsibly. I will not use computers, handheld computers, digital audio players, cell phones, personal digital devices or the Internet to send or post hate or harassing mail, pornography, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors either at school or at home.

I understand that I represent the school district in all my online activities. I understand that what I do on social networking web sites such as Snapchat, Instagram and Facebook should not reflect negatively on my fellow students, teachers, or on the FHCS community. I understand that I will be held responsible for how I represent myself and my school on the Internet.

I **will not** attempt to alter, change, modify, repair or reconfigure computer and mouse settings, the background properties or any other settings of the computer I use unless it is with the express prior permission of a staff member.

I **will not** attempt to gain access to another person's files or purposefully damage another's work.

I **will not** damage hardware, software, or other computer or school equipment intentionally.

I **will not** attempt to break into restricted areas of any computer or the school network.

I **will not** install programs, apps, or CDs (music or software compact discs) brought from home or downloaded off the Internet unless I have a staff member's permission, including browser plugins and extensions.

Internet

I **will** use the Internet educationally in order to explore, develop and care for God's world.

I **will** use the Internet only with a staff member's permission and/or supervision.

I **will** not use any "incognito" browsing window that makes user activity untraceable.

I **will not** delete any cookies, bookmarks or history from a school computer or change the date/time.

I **will not** view, exchange, or download any files that are adult or pornographic in nature.

I **will** abide by copyright guidelines/laws. (No downloading media or illegal streaming.)

I **will not** access sites that are not approved.

I **will not** meet in person with anyone "met" using online resources, without parental or teacher supervision and in a public place.

I **will not** use the Internet for any activity that violates United States or local laws. This includes, but is not limited to, threatening the safety of another person, cyber bullying, or violating any laws.

Mobile Devices

I will not use my cell phone or mobile device during passing periods or during lunch.

I will keep my cell phone on silent and stored in my hallway locker and/or classroom bins. I will not carry or use my cell phone in bathrooms or locker rooms on campus.

I will take personal responsibility for all media I access, record, or share.

I have read and understand the above information about appropriate use of the computer network at Flint Hills Christian School. I understand that use of computers and the school network is a privilege, not a right. I understand that this form will be kept on file at the school. I am prepared to be held accountable for my actions and for the loss of privileges if the Acceptable Use Policy is not followed.

_____ _____ _____ _____

Student Printed Name Grade Level Student Signature Date

Parent/Guardian Permission

I have read and understood the above information about appropriate use of the computer network at Flint Hills Christian School. I understand that this form will be kept on file at the school. My child has permission to access the network as outlined above.

_____ _____

Parent/Guardian Signature Date

Students and parents will sign an acceptable use policy each year. The administration is responsible for monitoring compliance with the policy.

Computer User Agreement for FHCS K-5 Students

1. I **will not** damage the computer or network in any way.

2. I **will not** use a computer or hand-held device to harm other people or their work.

3. I **will not** violate copyright laws.

4. I **will not** view or use other people's folders, files or work without their permission.

5. I **will not** view, send or display offensive messages or pictures, or harass others in any way.

6. I **will not** access any personal accounts free e-mail/communication services from any school computer. This includes email, social media, and gaming accounts and applies to time in PM Academy.

7. I **will not** send a person my picture or any personal information, such as name, address, etc., about myself without first checking with my parents or teacher.

8. I **will not** view Internet sites that my school or teacher does not allow, or thinks are inappropriate.

9. I **will not** represent other people's work as my own (plagiarism).

10. I **will** tell any adult immediately if I see materials that violate these rules.

11. I **understand** that all electronic files are subject to review by the administration.

12. **I will** tell a parent or a teacher right away if I come across any information that makes me uncomfortable.

13. **I will** never get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will make sure it is in a public place and I will bring my mother or father along.

I am prepared to be held accountable for my actions and for the loss of privileges if the Acceptable Use Policy is not followed.

Student's signature _____

or

Parent's signature _____

Students and parents will sign an acceptable use policy each year. The administration is responsible for monitoring compliance with the policy.

Appendix

This material in this document was either copied or adapted for FHCS from the Acceptable Use Policies of the schools and organizations shown below. The policies of many other schools were also reviewed for comparison./

Brookfield Christian School (https://www.brookfieldchristian.org/wp-content/uploads/2015/11/BCS-Student-AUP-8.3.16.pdf)

Cair Paravel Latin School (http://www.cpls.org/family/wp-content/uploads/2012/03/CPLS-Student-and-Family-Handbook-For-Final-Printing-1.pdf)

Catholic Diocese of Arlington (https://saintrita-school.org/wp-content/uploads/acceptable-use.pdf)

Christian Brothers Academy (https://www.cbalincroftnj.org/wp-content/uploads/2018/07/2018-CBA-Tech-Acceptable-Use-Policy.pdf)

Conway Christian School (http://www.conwaychristianschool.org/academics/acceptable-use-policy.cfm)

Corn Bible Academy (http://www.cornbible.org/Websites/corn/images/2017%20Handbook.pdf)

Cushing Academy (www.cushing.org/academics/technology/acceptable-use-policy)

FCC Children's Internet Protection Act (CIPA)

Getting Started on the Internet: Developing an Acceptable Use Policy (AUP), Education World, https://www.educationworld.com/a_curr/curr093.shtml

Getting Started on the Internet: Safe Surfing, (https://www.educationworld.com/a_curr/curr073.shtml)

Google "Be Internet Awesome" Curriculum (https://beinternetawesome.withgoogle.com/en_us)

Heritage Christian School (https://docs.wixstatic.com/ugd/2616bc_2b4f1e96a5414917a3691392b7c5befc.pdf)

Starkville Academy (https://www.starkvilleacademy.org/editoruploads/files/2018-2019_Handbook_Updated(1).pdf)

Trinity Academy (http://trinityacademy.org/wp-content/uploads/2015/07/2015-16-Parent-Student-Handbook-final-for-Planner.pdf)

Twin Tiers Christian Academy (http://www.twintierschristianacademy.org/technology-use-policy.html)

Valley Christian School (https://static1.squarespace.com/static/54b1749ae4b05d6e3b8949e3/t/5bb3d3a953450a1e7e693279/1538511788928/parent-handbook-2018-19.pdf)

Who We Are Together, Not Apart, https://www.educationworld.com/a_tech/columnists/guhlin/guhlin010.shtml