St. Hugh Catholic School

2022 – 2023

Acceptable Use Policy ("AUP")

STUDENT NAME: _____ DATE: _____

Homeroom Teacher: _____

St. Hugh Catholic School is committed to student use of technology as a tool to expand learning opportunities and conduct scholarly research. The use of technology facilitates global collaboration--a vital skill for our 21st century learners. Students at St. Hugh Catholic School utilize devices on a wireless network. Devices and the wireless network on the St. Hugh Catholic School campus are strictly for educational use consistent with St. Hugh Catholic School's educational goals. Along with the opportunity this provides, comes responsibility. This Acceptable Use Policy is designed to give the student and the student's family, as well as others on the School's campus, clear and concise guidelines regarding the appropriate use of devices. The underlying premise of this policy is that all members of the St. Hugh Catholic School community must uphold the values of honesty and integrity. We expect our students to exercise good judgment and to utilize technology with integrity.

Gaggle Safety Management -formerly Human Monitoring Service (HMS) – removes the need for educators to review questionable communications so that they can concentrate on classroom instruction. Gaggle's Safety Management greatly improves the safety and security of students, both online and in the real world, by having a trained team of Student Safety Representatives monitor student content 24/7.

Email

- The use of email during class is prohibited unless authorized by faculty or administration on a case by case basis.
- Students are not allowed to have any personal accounts in their iPad for example: iTunes, personal email accounts and others.
- Students should always use appropriate language in their email messages.
- Email services provided by the school are to be used only for the exchange of appropriate information.
- Students are to use only Gaggle email as a mean of email communication.
- No inappropriate email will be tolerated, including derogatory, obscene, or harassing messages. Email messages of an abusive or harassing nature will be regarded as a major violation and will be subject to a disciplinary response, which may result in expulsion.

- Chain letters of any kind and spam are prohibited. Chain letters are defined as any email message asking you to pass information or messages on to other individuals or groups via email.
- Students are prohibited from accessing anyone else's email account without first receiving explicit permission from the account holder. Email etiquette should be observed. In general, only messages that one would communicate to the recipient in person should be written. Only approved email programs may be used for student email.

- School email addresses are not to be given to ANY websites, companies, or other third parties explicitly unless authorized by faculty or administration on a case by case basis.
- Only school-related attachments may be sent on the school email system.

Social Media and Blogging

- Instant messaging is prohibited on campus except as part of an assigned, in-class activity that is supervised by faculty or administration.
- Blogging is to be utilized on campus, only for academic purposes.
- Participation in social Media networks during school hours is prohibited during the school day, except as part of an assigned, in-class activity.
- Clubhouse (consists of live audio);
- Reels (video, similar to Tik Tok), along with highly used Instagram, Snapchat and Tik Tok or other similar.

Sexting

- The electronic transmission or receipt from one minor to another of any photograph or video that depicts nudity may constitute illegal sexting. Students engaged in sexting will be subject to serious disciplinary consequences which may include administrative withdrawal from school. In addition, the school administration may report instances of sexting to the Florida Department of Children and Families or local law enforcement for appropriate investigation as to violations of law. The electronic transmission of sexually explicit language by a student may also constitute grounds for disciplinary action.

Audio Camera and Video

- Audio should be turned off or on silent unless required for the activity being conducted.
- Listening to music either aloud or with earphones is not permitted on campus unless required for the activity being conducted. Faculty and staff may relax this policy at their discretion.
- When sound is needed, headphones provided by the student must be used.

- Camera is disable unless required by a teacher.
- The use of devices to watch movies and DVD videos, unless assigned by a teacher, is not permitted during the school day.
- Any audio or video recording may be done only with the prior permission of all parties being recorded.
- Sharing of music (including iTunes music sharing) over the school network is strictly prohibited and is subject to disciplinary action.
- YouTube can only be used for educational purpose.

Games

- The viewing and/or playing of electronic games is not permitted during school hours, except as part of an assigned, in-class activity.
- The school reserves the right to remove any game from a school device that is considered inappropriate or impedes the educational purpose of the program.
- **No games that are played over the school network are allowed.**
- Games that include violence, adult content, inappropriate language, and weapons are not to be installed or played on the devices.
- Screensavers that include gaming components are not allowed.

Devices

Student devices must not be left unattended at any time. If a device is found to be unattended, it will be turned in to the Technology Office.

- Devices must be in a student's possession or secured in a locked classroom or locker at all times.
- Do not lend your device to other students.
- Do not borrow a device from another student.
- Devices must be carried and transported appropriately on campus. They should be carried in their approved cases at all times. Failure to do so could damage the screen.

  Note: Students are entirely responsible for backing up their own data. Lost or damaged data is not the school's responsibility. All school-issued devices must be in the school-issued device case or one that completely encases the device with special protection to the device's corners.
- Do not consume food or beverages near the devices.
- Devices should be handled with care. Inappropriate treatment of school devices is not acceptable.
- No writing or stickers will be allowed on the device and device cases, and these are not to be defaced in any way.
- Do not remove, move, or write on the identification sticker on your device.
- Students are not allowed to create any administrative passwords on their devices.
- Students are expected to come to school with a fully charged battery on a daily basis. **If not**, a loaner will be supplied to the student and a charge of **$25.00** will

be applied. (Any unpaid balance may result in holding the report cards, Plus Portal reports or transcript).

Network Access

- Students must not make any attempt to access servers or network information that is not available to the public.
- The utilization of proxy avoidance IP numbers and programs is strictly prohibited.
- Students may not use the school network for personal or private business reasons including but not limited to online ordering and purchases.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal law (Florida iPad Crimes Act, Chapter 815, Florida Statutes). This includes tampering with iPad hardware or software, vandalizing data, invoking iPad viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.
- The School is not responsible for damaged or lost data transferred through our network or stored on devices or our file servers.
- Students must be connected to StHughWeb for the WiFi at all times in school.

File Sharing

- File sharing is the public or private sharing of data or space. Any program that creates a point-to-point connection between two or more computing devices for the purpose of sharing data is considered file sharing.
- File sharing of any kind is prohibited both on campus and off campus. The only exception to this is when it is a specific assignment given by a faculty member.
- There is a $25 reimaging charge to remove any unapproved apps or files. **This amount may be increased for repeat violations.**

Deleting Files

- Do not delete any folders or files that you did not create or that you do not recognize. Deletion of certain files will result in device failure and will interfere with your ability to complete class work and may affect your grades.
- There is a $25 reimaging charge to correct system files. **This amount may be increased for repeat violations.**

Downloading and Loading of Apps or Software

- Students are not permitted to install custom/individual applications that require administrator privileges.
- All installed Apps must be done through the MDM.
- The downloading of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
- The school reserves the right to remove any apps that has been loaded onto the device that impedes the educational purpose of the device program.

- Copyrighted movies may not be "ripped" from DVDs and placed on the devices nor may copyrighted movies be downloaded to the devices from the Internet.
- Only commercial videos (such as television programs) legally purchased from the iTunes music store or another like entity may be downloaded to the devices.
- There is a $25 reimaging charge to remove any unapproved software or files. **This amount may be increased for repeat violations.**

Screensavers

- Inappropriate or copyrighted media may not be used as a screensaver.
- Pictures or videos which include the presence of weapons, pornographic materials, inappropriate language, alcohol, drug, gang-related symbols or pictures will result in disciplinary actions.
- There is a $25 reimaging charge to remove any of the above. **This amount may be increased for repeat violations.**

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 items of a sexual or pornographic nature, extremist or militant materials, gambling, depictions of violence, images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.
- Information obtained through the Internet must be properly cited and in compliance with 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 resources will be treated in the same manner as any other incidences of plagiarism.
- If a student accidentally accesses a website that contains obscene, pornographic or otherwise offensive material, he/she is to notify a teacher, the Executive Director of Technology, or the Technology Coordinator as quickly as possible so that such sites can be blocked from further access. **THIS IS NOT MERELY A REQUEST; IT IS A RESPONSIBILITY.**

Privacy, Use, and Safety

- Students may not give any personal information regarding themselves or others through email or the Internet including name, phone number, address, passwords, etc. unless they are completely 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 email address or other personal information regarding other students, faculty, or administration to anyone outside of the school without their permission.
- Students must secure and maintain private passwords for network and device access. This is important in order to protect the privacy of each student. **Do NOT share personal passwords or usernames.**
- The School respects the privacy of every student, faculty member, and administrator with respect to stored files and email accounts. However, if inappropriate use of email accounts or the School's network, including student/faculty handbook violations or harassment, is suspected, the school's administration has the right to view these files in order to investigate suspected inappropriate behavior.
- The school will monitor iPad activities, including logging website access, newsgroup access, bandwidth, and network use.
- Students are prohibited from accessing faculty, administration, and staff files servers for any reason without explicit permission from the user or administrator of that iPad.
- Students are prohibited from utilizing peer-to-peer networking or any method of file sharing unless authorized by the technology staff.
- No identifiable photographs of students, faculty, or administration will be allowed to be published on the Internet or used in print without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.
- Cyber-bullying is the use of electronic information and communication devices to willfully harm a person or persons through any electronic medium, such as text, audio, photo, or video. Examples of this behavior include, but are not limited to:
    - Sending/posting false, cruel, hurtful or vicious messages/comments;
    - Creating or contributing to web sites that have stories, cartoons, pictures, and jokes ridiculing others;
    - Breaking into an email accounts and sending vicious or embarrassing materials to others;
    - Engaging someone in electronic communication, tricking that person into revealing sensitive personal information and forwarding that information to others;
    - Posting of a student picture without their permission.
- Any electronic communication that creates a hostile, disruptive environment on the school campus is a violation of the student's and of the staff member's right to be safe and secure. Actions deliberately threatening, harassing, or intimidating an individual or group of individuals; placing an individual in reasonable fear of harm; damaging an individual's property; or disrupting the orderly operation of the school will not be tolerated.
- Devices that are provided by the school continue to be the property of the school. Therefore, the school has the right to view all content at any time.

- Any electronic device used on the school network, even if privately owned, is subject to all policies and consequences of the AUP including: the right to view the content of the device at any time; the right to remove content from the device; and the right to retain the device in the school's possession if there is an infraction to the AUP that deserves that consequence, as determined by the School's administration.

Copyright

- Unauthorized duplication, installation, alteration, or destruction of data programs, hardware, or software is prohibited.
- Data, programs, hardware, software, and other materials including those protected by copyright may not be transmitted or duplicated.

Unacceptable Use of Outside Technology

The school expects students to use information technology (including, but not limited to, the Internet, email, instant messaging and text messaging) in a responsible and ethical fashion in compliance with all applicable laws and with Christian moral principles, both in and out of the school setting. Accordingly, students may not post, place, upload, share, or communicate any images, photographs, statements or inferences relating to or including profanity, vulgarity, indecency, illegal use of drugs, illegal use of alcohol or other illegal or illicit activities. Additionally, students may not use information technology for the purpose of defaming, threatening, teasing or harassing any other student, staff member, parent, faculty member, or other person. This includes, but is not limited to, communications on social networks such as Instagram and Facebook. In addition, this rule applies to communications both during the school year and while students are on vacation or summer breaks. Students are responsible for all materials and communications made on personal websites and social networks and the materials and communications should be consistent with Christian moral principles, including any materials or communications posted on their sites by other individuals. Moreover, any unauthorized use of the school's name (or common names associated with the school) or any likeness or image of the school or its employees or agents is strictly prohibited.

Consequences

- The school reserves the right to enforce appropriate consequences for the violation of any section of the AUP. Such consequences could include the loss of the privilege to use an iPad, the loss of the use of the iPad for an amount of time determined by the administration and members of the Technology Department, possible disciplinary action and possible legal action.

- These consequences apply to students participating in the Apple iPad program at the School as well as to students who are using the school's iPad off campus.
- Any device with illegal or inappropriate software or materials on it will be reformatted or "reimaged," and the student will be charged a $25 AUP violation fee PER incident for this service. **This amount may be increased for repeat violations.**
- In the case of repeated device abuse and/or damages, the school has the right to revoke the use of the school's device and the student will be restricted to using it only on campus. Repeated AUP offenses or device abuses may lead to the loss of a student's privilege of using a device on campus.
- Students are to report any known violations of this AUP to appropriate administrative staff members. **Random checks of student devices will be conducted throughout the year to ensure that these policies are being followed**.
- The School takes no responsibility for activities conducted on the devices or materials stored on the devices, or the school's network.

St. Hugh Catholic School

2022 – 2023

Acceptable Use Policy Acknowledgement Receipt Form

Disclosures: The student and the student's parent or guardian, hereby agrees to the terms of this Student iPad Use Liability Agreement and the Acceptable Use Policy.

I acknowledge that I have read the entire contents of the iPad Use Liability Agreement and Acceptable Use Policy and understand the consequences of any violations of the rules and policies of the school.

I agree to cooperate with the school in the interpretation and enforcement of the policies outlined in the Acceptable Use Policy. I also understand that the school has the ultimate authority over the administration of the school and the interpretation of the school's rules and policies. Moreover, I further understand that all of the school's policies whether written or verbal are only guidelines and are subject to change at the sole discretion of the school with or without notice.

I also hereby acknowledge that I have read and agree to the terms of the **RELEASES** outlined in the iPad Use Liability Agreement and Acceptable Use Policy.

Student Name _____

Student Signature _____ Date _____

Parent Name _____

Parent Signature _____ Date _____

_____ _____

Principal or Asst. Principal Signature Date