Holy Cross School
Technology Policy Guide

Primary Campus
5601 Elysian Fields Ave., New Orleans, Louisiana 70122
Telephone: 504-942-1850

Middle and High School Campus
5500 Paris Avenue, New Orleans, Louisiana 70122
Telephone: 504-942-3100

Website: http://www.holycrosstigers.com

Holy Cross School is fully accredited by the Louisiana State Department of Education and the Southern Association of Colleges and Schools as a college preparatory school for boys, grades Pre-K through 12.

The rules set forth in this policy guide may be amended.
The most current version of the Technology Policy Guide will be maintained on the school website.

Rev. June 2020
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holy Cross Acceptable Use Policy</td>
<td>3</td>
</tr>
<tr>
<td>Student Technology Guidelines:</td>
<td></td>
</tr>
<tr>
<td>Bring Your Own Device (“BYOD”) Laptops</td>
<td>5</td>
</tr>
<tr>
<td>Minimum and Recommended Specifications for BYOD Devices</td>
<td>7</td>
</tr>
<tr>
<td>BYOD Frequently Asked Questions</td>
<td>8</td>
</tr>
</tbody>
</table>
Holy Cross School Acceptable Use Policy

Holy Cross School aims to foster personal growth in technology, information gathering and communications skills. The purpose of this Acceptable Use Policy is to foster the independent use of the school network, subject to procedures and standards for appropriate network behavior and communication. Holy Cross School reserves the right to monitor students’ use of technology, including personal messages and Internet usage.

Independent use of the school network is necessary for students to pursue educational goals. Such use is subject to the procedures and standards for appropriate network behavior. Therefore, the cooperation of all parties, including parents, is critical to ensure the appropriate use of technology. Violations of the Acceptable Use Policy (“AUP”) are deemed a major offense and will result in appropriate disciplinary action.

Students MAY NOT engage in any conduct that violates this AUP. Some specific examples include, but are not limited to, the following:

1. **Any attempt, by any means, to circumvent system security (e.g. Ultrasurf or similar program), bypass internet content filtering, guess passwords, or in any way gain unauthorized access to local or network resources is forbidden.** Violation of this policy will result in major disciplinary action as follows:
   - **Offense #1** – Saturday Detention
   - **Offense #2** – Suspension/Expulsion
   - **Offense #3** – Suspension/Expulsion
   - **Offense #4** – Suspension/Expulsion

   The School Administration reserves the right to randomly inspect student’s devices to ensure security measures in place are not being circumvented and that the student is using the device for educational purposes while on campus.

2. Transferring copyrighted materials to or from any Holy Cross School network without the express consent of the copyright owner. This is a violation of federal law and is expressly prohibited.

3. The primary use of the network shall be reserved for those individuals utilizing materials that have a direct or indirect impact on the student’s educational program at Holy Cross School. Network use for e-mail to friends, chatting, reading jokes, searching sport sites, farming out information on games, or other actions that are not directly or indirectly related to the School’s curriculum are not of educational value and are not allowed.

4. Any use of the system, including the Internet and e-mail, for defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, illegal or other prohibited material is not permitted. Use of the system to harass, defame, or offend is forbidden. Individuals are encouraged to report any such misuse of the system to the Director of Information Technology.

5. All users must recognize that e-mail or network messages may contain thoughts, conclusions, and certain biased perceptions that were never intended for publication. There may be liability for defamation or spreading false and disparaging information about third parties, particularly comments on students, personnel applicants, or various vendors. Such use of the network is expressly prohibited.
6. No personal or student information, which is protected by the Family Educational Rights and Privacy Act, shall be disseminated through the network.

7. All users of the network must comply with the Electronic Communication Privacy Act (ECPA), Child Internet Protection Act (CIPA) and may need to comply with the Communications Decency Act (CDA). These Acts prohibit the unauthorized interception or disclosure of e-mail messages by third parties, and govern the appropriateness of certain material being remitted to the Internet. The ECPA does permit interception or disclosure if either the sender or the receiver of the communication consents.

8. No student should ever give out his own, or someone else's name, address, or telephone number to strangers online or anywhere else.

9. Users of the network recognize that the School does have the authority to intercept e-mail messages of all users and acknowledge that no privacy right is construed to exist in the network. The School Administration reserves the right to monitor all accounts by any means whatsoever, with or without the user’s knowledge, to determine that the network is being used for educational purposes and in compliance with these Guidelines.

10. Network users may never share their password with another person or allow another person to share their account. It is the user’s responsibility to protect accounts from unauthorized use, including changing passwords periodically and using passwords that are not easily guessed. Students are not allowed to log onto another student’s laptop or to use another student’s login and password on their computer. Logging onto the network with another student’s ID and password or using another student’s computer constitutes hacking and will result in major disciplinary action.

11. Use of the Internet for commercial gain or profit is not allowed from the Holy Cross network.

12. Users may not move, open the case of, or reconfigure any school-issued computers. Users are financially responsible for any damage they cause to a computer or any segment of the network.

13. Students may not attempt to harm or destroy property of Holy Cross School, another user, or any other agencies or networks that are connected to the Internet. In addition to physical damage inflicted to equipment, this policy includes, but is not limited to, the uploading, downloading, or creation of computer viruses or other programs designed to damage computers, attempts to crash computers or networks, and attempts to bypass security arrangements and programs. Security on any computer system is a high priority because there are multiple users whose work is often the product of many hours of effort. Any student who identifies a security problem should notify the School at once and must not demonstrate the problem to other users.

14. Holy Cross School makes no warranties of any kind, whether expressed or implied, for the services it is providing. The School will not be responsible for any damages suffered while using the system. These damages include, but are not limited to, loss of data because of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or the user’s errors or omissions. Use of any information obtained via the information system is at a user’s own risk. Holy Cross School is not responsible for the accuracy of any information obtained through electronic information resources.

15. Removable flash drives may be used at school, only if they contain data or information for a class or project. Flash drives are not to have stored on them any type of program or material that would be considered in violation of school policies (examples include games, hacking software, tweaks, and music.)

16. Under no circumstances is a student to use a computer designated as a faculty or administrative staff member’s computer. **There are no exceptions to this regulation.**

17. Students are not allowed to use the school logos, Crest, or any other graphic representation that is specific to Holy Cross School without the permission of Public Information Officer.
18. Students should not publish or cause the publishing of material to the internet that in any way is offensive, inappropriate, or in any way may cause harm to Holy Cross or its faculty, staff or students. This includes but is not limited to material posted on personal websites, social networking sites, forums, or blogs.

19. Students are not allowed to use any Holy Cross School material, including information from the Holy Cross website or Holy Cross promotional materials, on personal web spaces or social networking sites.

Student Technology Guidelines: Bring Your Own Device (“BYOD”) Laptops

Internet Safety Education
Holy Cross joins federal, state and local agencies along with our parents in educating our students about internet safety, interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response. Holy Cross provides education at all grade levels using the isafe.org curriculum. Parents can gain additional information regarding this program at www.isafe.org. In addition to the isafe program, Holy Cross engages at times guest speakers from law enforcement agencies to present Internet Safety to all our students.

Specific Guidelines for BYOD Program
Students in grades 5-12 for the 2020-2021 school year are required to provide their own laptop device that meets the minimum specifications outlined on the Holy Cross website. Students must have their laptops charged and ready for use at all times for classroom work. The school requires that all laptops have an acceptable level of functionality.

The maintenance and care of any device brought onto the school site remains the sole responsibility of the student and his family. Any damage or loss remains the responsibility of the students, and the school accepts no liability in such cases.

The use of personal devices is a privilege, not a right. The use of personal technology entails personal responsibility. It is expected that students will comply with the Holy Cross Acceptable Use Policy, act in a responsible manner, and honor the terms and conditions set by the classroom teacher and the school. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary action.

General:
The following are general guidelines recommended for keeping personal devices safe and to avoid damage that could occur from improper use and storage:

- Laptops should be kept on a flat surface when powered up and should be properly shut down before closing the lid.
- Failure to shut down when closing the lid will cause the laptop to overheat and become damaged.
- The laptop should not be moved while powered up. The laptop hard drives are extremely delicate, and any movement can cause failure.
- Under no circumstances should students walk around with their laptops on and screens open.
- Students should save all work to their “Documents” folder or directly to their network drive (SSWEB).
- Students are to store their laptop in their Holy Cross book bag when the laptop is not in use. The Holy Cross book bag is the only bag allowed on campus.
- Students should keep their laptop with them at all times. When this is not possible, students should secure their laptop in their assigned locker or a secured room. Students should make sure their laptop is powered off before storing.
**Laptop Power:** Students are responsible for charging their laptop batteries at home each night. Power outlets are not to be used in the classrooms for the purpose of charging laptop batteries. Particular care should be given to the power adapter and its storage. Wires wrapped too tightly can cause kinks and will result in a failed power brick.

**Email:** Students will be assigned an hctigers.org email address. The use of the Holy Cross email address must be used for educational purposes only. Students are not allowed to forward their other email accounts (Hotmail, Gmail, yahoo, etc.) to their Holy Cross email address. The network will automatically monitor all emails for executables and messages carrying viruses. The use of a Holy Cross email account is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Under no circumstances are students allowed to send email blasts to the entire school or individual grade levels or special groups that are setup on the mail server. Students will be given limited storage for emails on the server and will be automatically warned when they near storage limits. Student email is cleared out at the end of each school year.

**Audio:** Because computer audio can be distracting and disruptive, the volume setting on the laptops should be completely turned off while students are on campus. Students may purchase headsets for classes that require audio.

**Video Files:** Only video files that are for a class assignment may be stored on the network drive. YouTube is allowed for educational purposes only under the direction of the teacher as to the videos students should access. Students are responsible for all copyright violations and penalties.

**Printing:** By using the network, students can print to any classroom printer, or to the library printers.
- Students should have their name on all material sent to a printer.
- Students should pick up all printouts within two hours of printing.
- Students are not to print to administration printers.

**Student’s Responsibility for Assignments:** Students should have their laptops available in and out of class and therefore are responsible for all assignments.

**Software:** The technology department working with the faculty determines the software programs that are loaded on student laptops. Therefore, students are not allowed to download and/or store copyrighted materials and/or programs on the laptop or network.

**Peer-to-Peer Software:** Use of peer-to-peer software is prohibited. This includes but not limited to uTorrent, BitTorrent, Soulseek, etc.

**Lost/Stolen Laptop:** Students bring electronic communication devices to school at their own risk, just like any other personal items. The school will not be held responsible if an electronic device or other item is lost, stolen or misplaced. Some devices have a device locator; it is recommended that you enable this feature if possible. In the event a student’s laptop is lost or stolen while on campus the student should report it immediately to the Dean of Boys or Dean of Men.

**Insurance:** Parents may wish to secure third-party insurance for the student’s laptop.
Minimum and Recommended Specifications for BYOD Devices

**Operating System**- Windows 10 64-bit (Home or Professional version 1909 or higher) for compatibility with Holy Cross wireless network, software and services, OR Mac OS X 10.15 or higher (MacBook, MacBook Air, MacBook Pro). Students who plan on taking AutoCAD should use Windows 10 64-bit OS. Chromebooks and iPads are not device options. Please be sure the computer has all the latest manufacturer and Windows updates.

**Battery life**- 5-hour minimum with 6+ hours recommended. Batteries cannot be charged on campus for safety considerations. A second spare battery is recommended but not required if your device has a removable battery.

**Cellular**- Devices are not allowed to have cellular access.

**Screen Size**- A minimum of a 12-inch screen is required.

**Keyboard/Mouse**- An attachable keyboard is required. When deciding please remember students will write papers in most classes. Most laptops come with an integrated trackpad but an external mouse (wired or wireless) may also be purchased if desired.

**Memory**- 6GB is the minimum recommendation with 8GB or 12GB suggested but not required. 8GB of RAM is the minimum recommended for students who plan to enroll in AutoCAD classes.

**Processor**- Equivalent to Intel i5 or i7. Intel and AMD are the top two processor manufacturers.

**Hard Drive/Storage**- A minimum of **128GB SSD (Solid-State Drive)**.

**Wireless Network Adapter**- **802.11ax or 802.11ac is required**.

**Software**- The device must be running licensed versions of all software, particularly operating system and anti-virus software. Student devices must have anti-virus software that has **real protection enabled** on the laptop prior to coming on campus. Some possible options include:

- Avast
- AVG
- Kaspersky
- Malwarebytes Antivirus
- McAfee
- Sophos
- Symantec and Norton
- TrendMicro

**Warranty**- Consider purchasing extra/extended warranty for accidental damage protection or to reduce further repair costs. It is important to know if the warranty work will be performed locally or require the device to be shipped to get repaired.

**Insurance**- You will need to check with your insurance company to determine the available options.
BYOD Frequently Asked Questions

1. Is my son required to have a laptop for school?
   Answer: Yes. The device will be used daily in class and for homework.

2. What are the minimum requirements for the laptop?
   Answer: Click here for the minimum and recommended specifications for BYOD devices.

3. What software are we required to have on the laptop/tablet?
   Answer: A legal version of the Windows 10 64-bit operating system (or Mac OS X 10.15 or higher) is required. Students will be required to install one of the school’s free licenses for Microsoft Office.

4. What are the guidelines for students transporting/storing their devices?
   Answer: Students are to store their laptop in their Holy Cross book bag when the laptop is not in use. The Holy Cross book bag is the only bag allowed on campus.

What happens if my son forgets his device at home?
   Answer: The laptop is an instructional tool that will be required in the classroom, just as a textbook, pen, and paper are required for the classroom, and will be subject to the same disciplinary measures.

5. How will the student’s laptop activity be monitored at home?
   Answer: Holy Cross monitors and controls student activity while at school. Ultimately, it is the responsibility of the parents to monitor their son’s activity at home.

6. Will my son be able to print at home?
   Answer: Yes. Your son will have administrative rights to his own device and can install printer drivers as needed from home.

7. Can my son add stickers or labels to his device?
   Answer: Students may not decorate, add stickers, etc. that could be considered offensive to others or that are not in accordance with the Catholic Church or the Holy Cross Man.

8. Who will repair the device if it breaks?
   Answer: The parent(s) are responsible for the repairs of the device. We encourage families to consider obtaining insurance and an accidental damage warranty for the device. The Holy Cross technology office can only provide minimal troubleshooting assistance to students who are having problems connecting to the school’s wireless network. Holy Cross School does not provide any mechanical repairs to student owned devices. It is not the responsibility of the teachers or staff to troubleshoot devices during the school day.

9. Will my son be able to access his files from home?
   Answer: Yes, your son will be able to access his files from anywhere that has an internet connection.
11. Is it required that my student use the school wireless network? Can they use their own 3G, 4G, 5G, LTE, or XLTE service?
Answer: The Holy Cross handbook states that all cellular and wireless capable devices must remain in the student’s locker during the school day. Any electronic or wireless communication device that is seen or heard will be confiscated and turned over to the dean of men, and the student will face disciplinary action. Equipment will be returned only at a parent conference. This includes smart watches. For the safety and security of our students, they are only allowed to use the school’s wireless network when accessing the internet from their device.

12. What if the device is lost or stolen?
Answer: Students bring electronic communication devices to school at their own risk, just like any other personal items. The school will not be held responsible if an electronic device or other item is lost, stolen or misplaced. Some devices have a device locator; it is recommended that you enable this feature if possible.

13. If a device runs out of power, can it be charged at school?
Answer: The school expects all student devices to be fully charged when brought to school. Charging personal devices at school is not allowed.

14. Are loaners available?
Answer: When personal computers are broken and need repair, loaner laptops are available under certain conditions:
- Parents/students must present proof that the personal computer is currently in repair before a loaner is issued
- Loaner laptops are only loaned before school and during school-scheduled breaks as students will not be allowed to miss class instruction to borrow a loaner laptop.
- Loaner laptops must be returned by the end of the school day, unless approval from the Dean of Boys or Men has been given for the loaner laptop to be taken home.
- Failure to return loaner laptops at the end of the school day or time noted by the appropriate Dean of Boys or Men will result in a per day charge of $25/day of delinquency and charged to the student’s SMART tuition account.
- Loaners must only be used for school-related work and must be connected to the Holy Cross WIFI at all times
- Parents are responsible for all damages to the loaner laptop.