HOLY CROSS
SCHOOL EST. 1849

Technology Guidelines and Use Policy for 2016-2017 release 1.1

Responsible Use Guidelines for Technology

Technology education at Holy Cross aims to foster personal growth in technology, information gathering and communications skills. Students using Holy Cross computers have the opportunity to access the Internet. The purpose of these Responsible Use Guidelines 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 the Internet usage, The following Responsible Use Guidelines apply to all users (faculty and students) when they access any school network connection. Violators of the Responsible Use Guidelines are subject to loss of access to technology or the Internet, and or other disciplinary action.

1. Independent use of the school network is necessary for students to pursue the educational goals of the School. 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 these Responsible Use Guidelines will result in disciplinary action.
   Consequences of network use violations include but are not limited to:

   1. Suspension or revocation of network privileges, computer access;
   2. School suspension or expulsion;
   3. Legal action and prosecution by the authorities.

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

3. The use of the Internet is a privilege. The primary use of the network shall be reserved to those individuals who are 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 students 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 may result in expulsion from Holy Cross.

11. Any attempt, by any means, to circumvent system security, 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 expulsion from Holy Cross.

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

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

14. 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.

15. 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 as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or your 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.

16. 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.)

17. Under no circumstances is a student to use a computer designated as a faculty or administrative staff member's computer nor should a teacher use a student's laptop. **There are no exceptions to this regulation**. Faculty members are not to use a student's computer for any reason.

18. Students are not allowed to use the school logos, Crest, or any other graphic that is specific to Holy Cross School without the permission of Director of Public Affairs.

19. 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.

20. Students are not allowed to use any Holy Cross School material, including information from the Holy Cross website on personal web spaces. (Example: Facebook, Twitter, Instagram, LinkedIn, etc...)

Internet Safety Education

Holy Cross joins Federal, State, & Local Agencies along with our Parents in educating our students with regards to internet safety, interacting with other individuals on social networking websites 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 guest speakers from the FBI to present Internet Safety to all of our Students.

Specific guidelines for Holy Cross laptops issued to students

Each 5th-12th grade student will be issued a laptop sometime during the school year as part of an initiative to support educational programs through the use of technology. The laptops are the property of Holy Cross and are to be returned after final exams at the end of the school year. All fines for damage to the computer must be paid before students will have access to final grades. If a student who has been issued a laptop computer leaves the school for any reason, the laptop and all accessories are to be returned and any fines paid before a transcript will be issued for the students.

General:

The school requires that all laptops have an acceptable level of functionality. If, in the opinion of the Director of Technology, a student machine has been adversely affected as a result of personalization, by the loading of inappropriate software or if inappropriate material has been stored on the hard drive, the school will re-image the computer and return it to the state in which the computer was issued to the student.

- 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 (U Drive). Additional instructions for this procedure and the synchronization of offline folders are available on the HC technology page of the website.

Laptop Storage:

- Students are to store their laptop in their Holy Cross Book Bag when the laptop is not in use.
- Students are not to store their laptop in any other case than their HC Book Bag.
- 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 Personalization & Software Installation:

- Students are not to personalize their laptops or install unauthorized software on their laptops. The addition of such material interferes with the efficient operation of the machine and is therefore affecting the efficiency of the use of the machine as an educational resource.

Laptop Power:

- Students are responsible for charging both of 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 holycrosstigers.com 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 holycrosstigers.com email address. The network will automatically monitor all emails for executables and messages carrying viruses. The use of a holycrosstigers.com 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.

Games:

- Games are strictly prohibited from being played on student laptops both on and off campus.

Music:

- Starting with the 2011-12 school year students are allowed to store a maximum of 75 songs on their laptop drive. Storage of inappropriate music will result in disciplinary action.

Video Files:

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

Hacking:

- Unauthorized use, or attempts to circumvent or bypass the security mechanisms of the network may result in the expulsion of the student. This includes attempts to bypass the internet content filtering.

Webcams:

- Unauthorized use or attempts to circumvent or bypass the security mechanisms of the network may result in the expulsion of the student. This includes attempts to bypass the internet content filtering.

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 print outs 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 the student laptops. Therefore, students are not allowed to download and/or store on the laptop or network copyrighted materials and programs.

Peer-to-Peer Software:

- Use of peer-to-peer software is prohibited. This includes but not limited to Imesh, Morpheus, Kazaa, WinMx, Limewire, etc.

Lost/Stolen Laptop:

- In the event the 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. A parent or guardian will be required to come to school to complete necessary paperwork.
- In the event the laptop is stolen off campus the parent/guardian is required to file a police report immediately. **The parent/guardian must submit the following information to the school on the next business day: Police item number, Police officer's full name, address of police district office (street, city, zip), and telephone number of district office.**
- There is an $800 charge for a replacement laptop. This charge is refunded if the laptop is recovered.

Financial Responsibility for lost/stolen equipment:

- The parent(s) and/or guardian(s) are financially responsible for the replacement value of any and all equipment lost or stolen. Current replacement cost is $1800 for the laptop plus reasonable attorney fees if the unpaid amount is turned over to an attorney for collection. Holy Cross maintains the right to change the replacement costs at any time. All current replacement costs will be posted on the HC website. Total payment for lost/stolen equipment is due four weeks after reporting incident or prior to student taking exams for the semester, whichever occurs first. A charge of $800 is due prior to a student receiving a loaner laptop while the incident is being investigated.

Financial Responsibility for student violation of agreement

- The parent(s) and/or guardian(s) are financially responsible for the cost associated with any and all repairs, network configuration changes, changes to network security, and all other costs associated with the student's violation of the Computer Use Policy.

Insurance:

- Parents may wish to secure third party insurance for the student's laptop. Should a claim become necessary, HC will provide parents with a report to file with their insurance company. However, the parent (s) and/or guardian are responsible for payment to HC for the lost, stolen, or damaged laptop.

Fee Assessment:

- Listed below is the price list for accidental damage to the computer. Payment is due at the time of service. Payment for damage may be made by cash or credit card online. Deliberate damage will result in the cost of repair plus disciplinary action taken by the Dean of Boys or Dean of Men.

Violation of Laptop Storage	$ 75.00
Re-imaging Charge	$ 75.00
Damaged Screen	$200.00
Damaged Keyboard	$ 45.00
Damaged DVD burner/player	$159.00
Damaged Memory Module	$100.00
Damaged/lost power adapter	$ 75.00
Damaged/lost battery	$159.00-$310.00 depending on model
Damaged/lost hard drive	$195.00
Bottom Base Cover Assembly	$100.00
Laptop Top Cover	$ 85.00
Cracked Casing	$ 85.00
Major dents, cracks, or scratches that impair operation	$30/hr labor plus cost of parts
Damage to mother board	$30/hr labor plus cost of motherboard
Other Minor/Major Damage	$30/hr labor plus cost of parts
Loss/Stolen laptop	$1800.00

Note: Pricing subject to change throughout the year based on Vendor's charge to Holy Cross. The most up to date version of this document is located on Edline.

Laptop Return Fee:

- A $100 fee will be charged for students not returning their laptop on the specified date/time. The laptop return dates are published at the beginning of 2nd Semester.

Students & Parents acknowledge acceptance of this policy when signing the School Handbook acknowledgment form.