ACCEPTABLE USE AND INTERNET SAFETY POLICY

(in accordance with Children's Internet Protection Act [CIPA])

PURPOSE: Hackett Catholic Central provides all students access to the Internet as a means to enhance their education. The purpose of this policy is to assure that students recognize the limitations that the school imposes on their use of these resources. In addition to this policy, the use of any electronic device used for school purposes also requires students to abide by the Hackett Catholic Central Schools Computer/Internet Acceptable Use Guidelines as stated in the Student Handbook and diocesan policies. During the course of the school year, additional rules regarding Internet safety may be added. If this occurs, any new rule will become a part of this policy.

TERMS OF THE ACCEPTABLE USE AND INTERNET SAFETY POLICY

Specifically, the student:

Should use the resources available through the Internet and other electronic media to supplement material available through the classroom, media center or through any other resource provided by the school.

Should adhere to guidelines each time the Internet is used at home and school. Social networking may be subject to evaluation by the administration.

Should make available for inspection by an administrator or teacher upon request any applications, messages, or files sent or received at any Internet location during the school day or in the context of school-related activities.

Should use appropriate language in all communications. The student should not use profanity or obscenity and should avoid offensive or inflammatory speech. The student should not participate in "Cyber Bullying" such as personal attacks and/or threats on/against anyone using these resources. The student should report to responsible school personnel any personal electronically transmitted attacks in any form made by others over the Internet or Local Area Network (LAN) observed while using school-owned or sponsored technology.

Should abide by copyright laws and should only download/import music or other files to a school-owned or personal computer, including laptops, tablets, or any electronic device used for school-related work, that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.

Should refrain from unauthorized electronic disclosure, use, or dissemination of personal identification information of minors. Exceptions to this is the required use of a student's real name in all educational activities that incorporate technology or the Internet (e.g., distance learning, online distance learning, etc.).

Should respect the privacy of others. The student should re-post (to make appear online again) communications only after obtaining the original author's prior consent.

Should use technology for school-related purposes only during the instructional day.

Should not make use of material or attempt to locate or transmit material via internet, electronic mail, or other forms of direct electronic communications that are unacceptable and inappropriate in a school setting. This includes, but is not limited to, pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or other materials. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school media center. Specifically, all school owned computers should be free at all times of any pornographic, obscene, graphically violent, or vulgar images, sounds, music, language, video or any other material deemed harmful to minors.

Should not download, upload, import or view files or websites that purport the use of illegal drugs, alcohol or illegal and/or violent behavior except school-approved, teacher-supervised digital media.

Should not access or attempt to access instant messages, chat rooms, forums, e-mail, message boards, or host personal web pages, except school approved, teacher-supervised filtered Internet communication, during the instructional day.

Should not attempt to discover passwords or to control access to the Internet or the computer network.

Should not change or attempt to change the configuration of the software or programs on school owned or sponsored equipment that control access to the Internet or any other electronic media.

Should not download any programs, files, or games from the Internet or other sources that can be run or launched on the computer as a stand-alone program. These programs or files are sometimes called “executable files.”

Should not use the interenet and electronic resources for any illegal activity. This includes, but is not limited to, using unauthorized access into computers, such as “hacking,” tampering with computer hardware or software, vandalism or destruction of computer files and any other unlawful online activity.

Should not knowingly introduce or knowingly allow the introduction of any computer virus to any HCC computer.

Should not connect a personal, non-school-owned desktop computer, laptop computer, wireless personal digital assistant (PDA), or any other network (wireless or directly plugged) device to any part of the HCC network (local area network “LAN,” wide area network “WAN," or wi-fi access) unless given express permission by a teacher or administrator.

Should access HCC's network only with his or her school assigned password, which should not be shared with anyone for any reason and should make every effort to keep all passwords secure and private.

Should not play games, including Internet-based games, except school-approved, teacher-supervised educational games, during the instructional day on any computer or electronic device.

Should not bypass or attempt to bypass HCC filtering software.

Will participate in and abide by all directives outlined in mandatory yearly student training that will be required as part of the school curriculum beginning in the 2012-13 school year. This training will cover the information in this Acceptable Use and Internet Safety Policy, as well appropriate behavior while online, on social networking Web sites, and in chat rooms.

I understand that should I fail to honor all the terms of this Policy, future Internet and other electronic media accessibility may be denied. Furthermore, I may be subject to disciplinary action	By signing below, I give permission for the school to allow my son or daughter to have access to the Internet under the conditions set forth above.
Student Name (Please Print)	Parent or Guardian Name (Please Print)
Student Signature	Parent or Guardian Signature
Date	Date