Acceptable Use Policy
St. Mary School, Shelby

I. Diocesan Statement on Technology

With Jesus, the Great Communicator, and in the spirit of our Christian tradition, we recognize that we live in a new media age, immersed in a new culture with an evolving language and method of communication. We propose to make use of the most effective means available to communicate the integration of faith and culture, which is at the center of Catholic values and education.

The use of new technologies presents new possibilities and challenges for the mission of the Church and Catholic education. The Church views emerging technologies as gifts of the Spirit to this age and challenges "God's faithful people to make creative use of new discoveries and technologies for the benefit of humanity and the fulfillment of God's plan for the world" (*Aetatis Novae, #2, #3; Rome, 1992*).

In keeping with the mission of the Catholic schools to promote values for a lifetime, the schools will instruct about and guard against inappropriate, unethical, and illegal use of the Internet by the student or adult user.

II. Introduction

The purpose of the Acceptable Use Policy is to clearly explain to students, parents, and school staff members the expectations that users of the system are expected to uphold. This document entails the practical considerations that need to be made by users of the system and carefully outlines exactly what practices are encouraged or forbidden by the school. The Acceptable Use Policy (AUP) gives students a clear statement of what is expected of them in terms of the day-to-day use of school technology and related services.

At ST. MARY'S SCHOOL, SHELBY, students are not allowed to have personal electronic devices on their person during the school day. If any such device is brought to school, it must be stored either in the locker or in a specific place as designated by the school. **See Family Handbook for infraction violation consequences.**

The following policy applies to school computers, technological devices, and network and is in effect whenever these are in use, on or off school property. Even if a user is using a school-issued computer after school, this policy still applies.

To gain access to school technology and the Internet, all students of St. Mary's School, Shelby must obtain parental permission and attend a series of required Internet training sessions. The signature(s) at the end of this document is (are) legally binding and indicate(s) the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

The following rules are provided so that everyone is aware of personal responsibilities. Any user in violation of these provisions may have his or her account terminated, and future access could be denied in accordance with the rules and regulations discussed during Internet training sessions. The school administration, faculty, and/or staff may request the Computer Teacher (or Technology Coordinator) to deny, revoke, or suspend specific user accounts.

III. Acceptable Uses

An acceptable use is one that is for educational purposes. The Computer Teacher (or Technology Coordinator), after consultation with the Pastor/President and/or Principal will deem if a particular use was acceptable, and their decision is final. However, it should generally be assumed that acceptable uses are academic in content and do not serve a purpose other than to enhance the education of a user.

A. **Safe Communication**
   1) *Personal Information:* When using the computer network and Internet, minors should not reveal personal information about themselves or any other individuals, such as home address, phone number, full name, or any other identifying information.

   2) *Meetings:* Minors should never arrange a face-to-face meeting with someone they first "met" online without seeking permission from the teacher and parent.

B. **Netiquette**
   1) *Behavior:* Users are expected to abide by generally accepted rules of network etiquette and conduct themselves in a responsible, ethical, and polite manner while online. Disruptive or disturbing behavior and the use of vulgar, obscene, or bigoted language or materials will be handled as disciplinary issues.

C. **Copyrights**
   1) *Honesty:* Users must respect all copyright laws that protect software owners, artists, and writers. Plagiarism in any form will not be tolerated.

IV. Unacceptable Uses

An unacceptable use is one that violates not only the specifics of the guidelines presented but the spirit of St. Mary's School, Shelby in keeping with its Internet Safety Policy and the teachings of the Catholic Church. It is possible that a specific use that is not discussed in the following guidelines is unacceptable since no list is completely exhaustive, so it is imperative that students act responsibly and are accountable for their actions. If a student is not sure if a particular use is permitted by the spirit of this policy, he or she should consult their teacher or Computer Teacher (or Technology Coordinator). Unacceptable uses will result in appropriate levels of discipline, possibly including a loss of computer access, as well as other disciplinary or legal action.

A. **Recording devices**
   1) *Messaging:* Students are not permitted to use any app that allows for transmission of videos or pictures that can be viewed only for a short amount of time (such as Snapchat).

   2) *Prohibited Areas:* Students may not take recording devices into certain areas such as bathrooms and locker rooms.

   3) *Sexting:* Students are not permitted to "sext" or transmit other sexually oriented images.

   4) *Permission:* Students may not use devices to record audio or video or to take pictures at any time without first obtaining permission from a teacher in advance. Permission will only be granted for the purposes of a bona fide school assignment.

B. **Downloads**
   1) *Games:* Students are not permitted to download or play games on school technology unless such game playing has an educational purpose and is specifically directed by the supervising teacher.

   2) *Viruses:* Students are not permitted to download (or upload) a worm, virus, Trojan horse, time bomb, or other harmful form of programming or vandalism.

C. **Unauthorized Access**
   1) *Bypasses:* Any unauthorized technology used for the purpose of bypassing security systems, avoiding internet filtering, or gaining unauthorized access is not permitted. This includes the use of ssh, proxy-bypass software, remote desktop sessions, anonymizing websites/software and other technologies.

2) *Other Accounts:* Students are not permitted to access another individual's account. Additionally, they are not allowed to delete, copy, modify, or forge other users' emails, files, or data, including online school resources such as Google Apps for Education, Microsoft Office 365, Powerschool, Edmodo, or Moodle.

3) *Mobile Hotspots:* Students are not permitted to use any device to create a mobile WiFi hotspot. This includes, but is not limited to, tethering apps and features on phones as well as portable WiFi hotspot technologies.

4) *Proper Action to Take:* If a problem does occur and the security of the school network is compromised, then users should notify a teacher immediately. Users should not demonstrate this problem to others.

5) *Internet Access*: Students are not permitted to connect to the internet through a source other than the school's specified provider. Accessing the internet via a 3G connection or otherwise is strictly prohibited.

D. Other Actions

1) *Employees:* Students should not email or post to webpages or blogs images, photos, or video of employees of the school. This includes the creation of fan pages or groups on social networking sites directed at a particular teacher or student (or a particular group of teachers or students) unless expressly authorized by the Principal.

2) *Online Activities:* Users are not permitted to use the resources for commercial purposes, product advertising, or political campaigning.

3) *Defamation:* Students are not permitted to create a fake account for the purpose of defaming another individual or person.

4) *Social Networking:* Students are not permitted to access social networking sites (such as Facebook, Twitter, Xanga, and Myspace) unless for academic purposes as specified by the supervising teacher.

5) *Tampering:* Users are not permitted to tamper (physically or electronically) with computer resources. Intentionally damaging computers, computer systems, operating systems, or computer networks will result in cancellation of privileges.

6) *Inappropriate Material:* Users are not permitted to transmit, receive and/or submit, or publish any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal materials.

7) *Cyberbullying:* Cyberbullying is strictly prohibited.

8) *Jailbreaking:* Students are not permitted to "jailbreak" school-provided devices (or do any similar process that wipes clean the hard drive of a device).

V. Content of Policy

A. Review and Revisions
1) *Current Policy*: Signed Acceptable Use Policies will be kept on file at St. Mary's School, Shelby.

2) *Updating the Policy*: Due to continuous advancements technology, additional restrictions and use guidelines may be instituted throughout the school year. If it becomes necessary to amend the Acceptable Use Policy, parents and students will be notified of the amendments.

   Retain this policy for your records. Return the signature page included on the registration form.