St. Margaret Mary Catholic School
Electronic Technologies Acceptable Use Policy

Network Use
St. Margaret Mary Catholic School network includes wired and wireless devices and peripheral equipment, files and storage, e-mail, websites, collaborative software, social networking sites, etc. Policies and procedures related to use of the school network resources includes access through school-owned and personally-owned computer/devices. The school reserves the right to prioritize access and use of the network. All network use is intended to support education and research and be consistent with the mission of the school.

Faculty, students, parents, and guests may be asked to sign a network use agreement before access to the school network or electronic resources is provided. The signed agreement will remain in force unless the parent notifies the school to revoke his/her child's privilege to access network resources or the user has violated school policies or procedures. Violations may result in the suspension or termination of network privileges and be subject to other disciplinary action according to school policies.

Connection of a personal electronic device to the district network by any person is voluntary and a privilege, and subject to all school policies and procedures.

The school assumes no liability or responsibility for any act of a staff, student or guest user that is inconsistent with school district policies and procedures. Any individual who brings personally owned devices onto school property is solely responsible for that equipment.

Responsible and acceptable use of technology by school network uses includes:

1) Creation of files, digital projects, videos, web pages and podcasts in support of education and research;
2) Participation in blogs, wikis, bulletin boards, Google sites, and groups and the creation of content for podcasts, email and web pages that support education and research;
3) The online publication of original educational material, curriculum related materials, and student work. Parental and student permission must be received in writing electronically or in hard copy before publishing student work. Sources outside the classroom or school must be cited appropriately;
4) Connection of personal electronic wireless devices to the school network is provided once faculty, parents, guests sign the Personal Device authorization form

and is accepted by the school administration. School staff will retain the final authority in deciding when and how students may use a personal electronic device on school grounds and during any school-related activity.

5) Faculty/staff use of the network for incidental personal use must be in accordance with all school policies and procedures.

Internet Safety

All students will be educated about appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

1) Age appropriate materials and resources will be made available for use across grade levels.
2) Training in or information about online safety issues and materials will be made available for staff, students and families.

Filtering and Monitoring

Filtering software through the school network and the Archdiocese of New Orleans network is used to block and/or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision made at the discretion of the school.

1) Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
2) Any attempts to bypass the school internet filter or conceal internet activity are prohibited such as, but not limited to, proxies, https, special ports, modifications to school browser settings and any other techniques designed to evade filtering or enable the publication or distribution of inappropriate content;
3) Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online must make a reasonable effort to monitor the use of this equipment to assure that students use conforms to the mission and goals of the school.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized school purposes. Students and staff are responsible for all activity on their account and must not share their account password.

No Expectation of Privacy

No student, staff, or guest user should have any expectation of privacy when using the school's network or electronic resources. The school reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate.