JESUIT HIGH SCHOOL
ACCEPTABLE USE TECHNOLOGY POLICY (2011-12)

General Usage Policies: As a Catholic college-preparatory school, Jesuit recognizes the need to educate young men and women to use technology ethically and effectively. Our technology goal is to encourage and enhance the use of 21st Century learning tools. We trust and expect that Jesuit students will use technology on and off campus in a manner consistent with the "Profile of the Graduate at Graduation" to become more intellectually competent, open to growth, and committed to doing justice. Students must:

1. **Respect and protect self and others.**
    - Not share personal passwords with others.
    - Use only assigned accounts, computers, and access rights.
    - Not view, use, hack, or copy passwords, data, or networks to which they are not authorized.
    - Not distribute private information about others or themselves.
2. **Respect and protect the integrity, availability, and security of all electronic resources.**
    - Recognize that the school's information technology resources, including email and internet access, are provided for educational purposes.
    - Observe all network security practices.
    - Report security risks or violations to a teacher or IT staff member.
    - Not intentionally destroy, damage, or attempt to damage data, networks, or other resources that do not belong to them.
3. **Respect and protect the intellectual property of others.**
    - Not infringe copyrights (including illegal copies of music, games, software, or movies)
    - Not plagiarize.
4. **Respect and practice the principles of community on and off campus.**
    - Communicate only in ways that are truthful and respectful of others.
    - Report threatening or discomforting materials to a teacher.
    - Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (including messages that are pornographic, threatening, rude, fraudulent, discriminatory, or harassing).
    - Not intentionally access, transmit, copy, or create material that is illegal (including obscenity, stolen materials, or illegal copies of copyrighted works).
    - Not use the technology resources, including Jmail and internet access, to further other acts that are criminal or violate the school's code of conduct.
    - Not send spam, chain letters, or other mass unsolicited mailings.
    - Not buy, sell, advertise, or otherwise conduct business using technical resources, unless approved as a school project.

Social Media: Social Media is defined as any electronic tool that allows for social, interactive, and connective learning allowing for but not limited to: video and photo sharing, social networking, blogs, wikis, podcasting, instant messaging, texting, web conferencing, or any other

technology that allows for direct or indirect interaction between two or more parties. When using social media, students are expected to observe and follow all policies listed above.
To maintain the professional relationship between students and faculty/staff members, the following policies will be followed when using social media to interact with students:

- Faculty/staff members will exercise good judgment when communicating with students via social media, including the use of appropriate language and visual images. Proper online behavior will be modeled by the faculty/staff member with special care to personal account privacy settings.
- If public social networks are used for classroom activities or club/programs, they will be monitored by the adult sponsoring the site. Monitoring will include, but not be limited to, the use of appropriate language and visual images, absence of cyber bullying, and adherence to academic purpose and US copyright laws.

Supervision and Monitoring: Jesuit reserves the right to impose consequences for inappropriate behavior that takes place on or off campus and outside school hours. Thus, inappropriate use of technology (for example, on a home computer), may subject the student to consequences. Inappropriate use includes, but is not limited to harassment, use of school name, remarks directed to or about teachers or other students, offensive communication, and safety threats. The school will monitor the use of technology resources to help ensure that users are secure and in conformity with the school's policy. Administrators reserve the right to examine, use, or disclose any data found on the networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of criminal activities to law enforcement.

Consequences for Violation: Violation of, or attempting to violate, these rules will result in disciplinary action as outlined in the school's handbook.