Introduction

It is the policy of St. Mary's Charter School ("School") to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA"). It is the goal of this policy not only to prevent and protect, but also to educate employees, students, parents and the School community in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by the School into its Acceptable Use Agreement.

The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet protection Act ("NCIPA") that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act, enacted October 10, 2008, adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

This policy is intended to be read together with the School's Acceptable Use Policies for Technology and the Internet. All limitations and penalties set forth in the Acceptable Use Polices are deemed to be incorporated into this policy. Terms used in this policy and that also appear in CIPA have the meanings defined in CIPA.[1]

---

[1] CIPA definitions of terms:

Technology Protection Measure. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **Obscene**, as that term is defined in section 1460 of title 18, United States Code;
2. **Child Pornography**, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

Harmful to Minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Sexual Act; Sexual Contact. The terms "sexual act' and "sexual contact" have the meanings given such terms in section 2256 of title 18, United States Code.

Compliance with the Requirements of CIPA

Technology Protection Measures

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. The School utilizes a sophisticated content filtering system that is compliant with CIPA and NCIPA on all computers that access the Internet.

Access to Inappropriate Material

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communication, access to inappropriate information. Specifically, as required by CIPA, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, technology protection measures may be disabled or, in the case of minors, minimalized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat, or circumvent the Technology Prevention Measures is punishable as a violating of this policy and of the Acceptable Use Policies.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the School's online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Acceptable Use Policies.

Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking" and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) to supervise and monitor usage of the School's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and CIPA. Procedures for the disabling or otherwise

modifying any technology protection measures shall be the responsibility of the Campus Principal or designee.

Education
The School will advocate and education employees, students, parents and the School community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, PTO/PTA presentations, and the School's website.

Cyber-Bullying
The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

The School is a place of tolerance and good manners. Students may not use the network or any School computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Network users may not use vulgar, derogatory, or obscene language. Network users also may not post inappropriate anonymous messages or forge e-mail or other messages.

Furthermore, the School computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas, or local laws. This includes, but is not limited to, any threat or act of intimidation or harassment against another person.