CARDINAL McCLOSKEY
COMMUNITY CHARTER SCHOOL

Internet Safety Policy

Introduction

It is the policy of the Cardinal McCloskey Community Charter School ("CMCCS" or the "School") to (a) prevent user access over its computer network which is intended to transmit or receive inappropriate material via the 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").

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 communications, access to inappropriate information. Although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board of Directors (the "Board") directs the Principal to procure and implement the use of technology protection measures that block or filter Internet access by:

- Adults to visual depictions that are obscene or child pornography, and
- Minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in CIPA.

Subject to staff supervision, however, technology protection measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Principal or their designee. Thus, for example, where warranted, access may be given to platforms like Facebook or Google.

The Principal or their designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using School computers; and restricting student access to materials that are harmful to minors.

Unauthorized/Inappropriate Network Usage

The Board of Directors (the "Board") prohibits the unauthorized disclosure, use, and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate material on the Internet and World Wide Web. Staff and students will be advised to not disclose, use, or disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.

To the extent practical, steps shall be taken to promote the safety and security of users of the CMCCS online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Social Networking Interaction & Cyberbullying

As part of this policy, the School shall also provide age-appropriate instruction regarding appropriate online behavior, including:

- Interacting with other individuals on social networking sites and in chat rooms, and
- Cyberbullying awareness and response.

Instruction will be provided even if the School prohibits students from accessing social networking sites or chat rooms on School computers.

Education, Supervision, and Monitoring

It shall be the responsibility of all members of the CMCCS staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, CIPA, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Operations or designated representatives.

All users of the School's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the School's acceptable use policies on the acceptable use of computers and the internet. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

The Director of Operations or their designee shall provide training for staff on the requirements of the School's Internet Safety Policy and regulation. The training shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.

The Director of Operations shall also provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include but not be limited to: (1) positive interactions with others online, including on social networking sites and in chat rooms; (2) proper online social etiquette; (3) protection from online predators and personal safety; (4) and how to recognize and respond to cyberbullying and other threats. Students shall be directed to

consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or the World Wide Web are directly related to their course work.

Following receipt of this training, the students/families will acknowledge that they received the training, understood it, and will follow the provisions of the School's acceptable use policies.

Staff and students will be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and regulation.

Internet Safety Regulation

The following rules and regulations implement the School's Internet Safety Policy adopted by the Board to make safe for children the use of School computers for access to the Internet and World Wide Web.

Definitions

In accordance with CIPA:

- *Child pornography* refers to any visual depiction, including any photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or (c) such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- *Harmful to minors* means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) 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 (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Blocking and Filtering Measures

The Director of Operations or their designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all School computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.

The Director of Operations shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the School.

The Director of Operations or their designee may disable or relax the School's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

The Director of Operations shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

Monitoring of Online Activities

The Director of Operations shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the School's Internet Safety Policy and this regulation. They may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the School's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the School's computer network shall have no expectation of privacy regarding any such materials.

Except as otherwise authorized under School policy, students may use the School's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.

Staff supervising students using School computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the School's Internet Safety Policy and this regulation.

The Director of Operations shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

Reporting Violations

Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Principal. The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures. Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of staff.

REVISED: 5/6/26