Board Policy – Internet Safety Policy

1. **Purpose**
    a. The Governing Board (Board) of Forest Ranch Charter School (FRCS) recognizes that staff and students have the right to work and be educated in a positive learning environment with clear rules for conduct for staff and students.
    b. FRCS provides and encourages the use of online resources for students, faculty, and staff. This policy attempts to ensure against improper system user exposure, retain data confidentiality, and maintain system security to the highest degree possible without preventing access to successful education practices, methods and materials.
    c. Therefore, it is the policy of the Governing Board of Forest Ranch Charter School to:
        i. ensure that students are educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyber bullying awareness, and response;
        ii. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
        iii. prevent unauthorized access and other unlawful online activity;
        iv. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
        v. comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].
2. **Responsibilities**
    a. The Director shall develop and implement appropriate documentation, training programs, and procedures to ensure compliance with this policy.
    b. Staff shall clearly convey school computer system procedures and rules to students, as well as the consequences of violation.
    c. Parents shall be provided a student Acceptable Use Policy to read with their students and ensure that the parents and students understand the importance of proper computer system use and conduct.

3. Access to Inappropriate Material

a. 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.

b. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

c. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

4. **Inappropriate Network Usage**

a. To ensure the safety and security of our system users, the public posting of personal information shall not occur. Contact information includes such things as name, physical address, telephone number, email address, and websites.

i. Chat rooms or other similar places on the internet shall not be visited.

ii. Students shall not agree to meet with someone they met online without parent or guardian approval and participation.

iii. Students shall promptly disclose to their teacher or other school employee any message they receive or site they visit that is inappropriate or makes them uncomfortable.

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

c. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

i. unauthorized access, including so-called 'hacking,' and other unlawful activities; and

ii. unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

5. Education, Supervision and Monitoring

a. It shall be the responsibility of all members of the FRCS staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet

Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

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

c. The Director or designated representatives will provide age appropriate training for students who use the FRCS Internet facilities. The training provided will be designed to promote FRCS's commitment to:

    i. The standards and acceptable use of Internet services as set forth in the FRCS Internet Safety Policy;

    ii. Student safety with regard to:

        1. safety on the Internet;

        2. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and

        3. cyber bullying awareness and response.

    iii. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

    iv. Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

d. The Director or designated representative will provide appropriate training and/or educational materials for staff, parents/guardians, and community members regarding the early warning signs of harassing/intimidating behaviors and effective prevention and intervention strategies.

6. Cyber Bullying

a. Cyber Bullying includes the transmission of communications, postings of harassing messages, direct threats, or other harmful texts, sounds, or images on the internet, social networking sites, or other digital technologies using a telephone, computer, or any wireless communication device. Cyber bullying also includes breaking into another person's electronic account and assuming that person's identity in order to damage that person's reputation.

b. The Board desires to prevent bullying and cyber bullying by establishing a positive, collaborative school climate and clear rules for student's conduct.

c. The School will provide students with instruction, in the classroom or in other settings, about appropriate online behavior and strategies to prevent and respond to bullying and cyber bullying.

d. The school staff will receive related professional development, including information about early warning signs of harassing/intimidating behaviors and effective prevention and intervention strategies. Parents/guardians, students and community members may also be provided with similar information.

e. Any student who engages in cyber bullying on school premises, or off campus in a manner that causes or is likely to cause a substantial disruption of a school activity or school attendance, shall be subject to discipline in accordance with school policies and regulations. If the student is using a social networking site or service that has terms of use that prohibit posting of harmful material, the Administrator or designee may file a complaint with the internet site or service to have the material removed.

7. Rules Violations

a. Employees are expected to provide appropriate supervision to enforce standards of conduct and, if they observe or receive a report of a violation of these standards, to immediately intervene or call for assistance. If an employee believes a matter has not been resolved, he/she shall refer the matter to his/her supervisor or administrator for further investigation.

b. Students who violate school internet safety rules and regulations may be subject to discipline including, but not limited to, suspension, expulsion, transfer to alternative programs, or denial of the privilege of participating in extracurricular or other school activities.

c. Staff members who violate school internet safety rules and regulations may be subject to discipline, up to and including dismissal.

d. The Director or designee shall notify local law enforcement as appropriate.

e. System users also may be subject to discipline, in accordance with law or Board policy, for any off-campus conduct during nonschool hours which poses a threat or danger to the safety of students, staff, or school property, or substantially disrupts school activities.

f. System users may submit a verbal or written complaint of conduct they consider to be bullying to a teacher or administrator. Complaints of bullying shall be investigated and resolved in accordance with Board Policy 3040 Uniform Complaint Policy.

    i. When a system user is suspected of or reported to be using electronic or digital communications to engage in cyber bullying against other system users, or to threaten school property, the investigation shall include

documentation of the activity, identification of the source, and specific facts or circumstances that explain the impact or potential impact on school activity, school attendance, or the targeted student's educational performance.

ii. System users shall be encouraged to save and print any messages sent to them that they feel constitute cyber bullying and to notify a teacher, the director, or other employee so that the matter may be investigated.

iii. If the system user is using a social networking site or service that has terms of use that prohibit posting of harmful material, the Director or designee may file a complaint with the Internet site or service to have the material removed.

8. Possession/Use of Cellular Phones and Other Mobile Communications Devices

a. No student shall be prohibited from possessing or using an electronic signaling device that is determined by a licensed physician or surgeon to be essential for the student's health and the use of which are limited to health-related purposes.

b. Students may possess, but not use, on school campus personal electronic devices including, but not limited to, pagers and telephones, digital media players, personal digital assistants, compact disc players, portable game consoles, cameras, digital scanners, and laptop computers unless expressly allowed on special days such as electronics day or as part of an approved class project.

c. Students using devices such as those mentioned above without permission shall have the devices confiscated and returned at the end of the school day.

9. Adoption and Review Timeline

a. This board policy was reviewed and adopted by the Forest Ranch Charter School governing board at a public meeting on June 14, 2012.

b. This board policy was reviewed and approved by the Forest Ranch Charter School governing board at a public meeting on March 21, 2023.

c. The next annual review will occur on or before March 21, 2024.