CIPA & FLORIDA COMPLIANT INTERNET SAFETY POLICY

NEWBERRY COMMUNITY SCHOOL, INC.

I. Purpose.

Newberry Community School, Inc., ("NCS" or the "School") recognizes the educational value of electronic devices, internet access, and online resources in supporting instruction, communication, research, and school operations. The School also recognizes that internet use presents risks to students, including exposure to inappropriate material, unlawful online activity, cyberbullying, unauthorized disclosure of personal information, and unsafe interactions with others through electronic communications. Accordingly, the Governing Board adopts this Internet Safety Policy to promote the safe and appropriate use of the School's internet access, online systems, and electronic devices, and to comply with applicable law, including the Children's Internet Protection Act ("CIPA").

II. Applicability.

This policy applies to students, employees, and other authorized users of the School's internet access, network, online systems, and School-issued devices. This policy applies when users access the internet through the School's network, through School-provided internet access, by using School-issued devices, or by using any device, including a privately owned device, connected to School-provided internet.

III. Technology Protection Measure.

To the extent practical, the School shall enforce the use of a technology protection measure, including an internet filter or similar technology, on all computers and other devices with internet access that are owned, leased, or controlled by the School and used by students or staff, and on any device regardless of ownership, that is connected to School-provided internet to the extent required by law and technologically feasible. The technology protection measure shall be designed to block or filter access by both minors and adults to visual depictions that are obscene or constitute child pornography, and to block or filter access by minors to visual depictions that are harmful to minors. The School shall also use technology protection measures to filter or block access to material that is not appropriate for students, taking into consideration the subject matter and the age of the students served. The School may also block or restrict additional categories of content that are inappropriate for the school environment, inconsistent with the School's educational mission, or otherwise prohibited by law or School policy. Subject to applicable law and administrative controls, the technology protection measure may be disabled or minimized for use by adults for bona fide research or other lawful purposes.

IV. Internet Safety Requirements.

The School's internet safety practices shall address each of the following:

1. access by minors to inappropriate matter on the internet and the World Wide Web;

2. the safety and security of minors when using electronic mail, chat rooms, messaging platforms, social networking websites, and other forms of direct electronic communication;
3. unauthorized access, including so-called hacking, and other unlawful online activities by minors;
4. unauthorized disclosure, use, and dissemination of personal information regarding minors; and
5. measures designed to restrict minors' access to materials harmful to minors.

V. General User Requirements.

Use of the School's network, internet access, and electronic resources is a privilege, not a right. All users shall conduct themselves in an ethical, responsible, lawful, and educationally appropriate manner. Users shall comply with the following requirements:

1. All use of the School's network and internet access must be for educational, instructional, administrative, operational, or other School-authorized purposes.
2. Users shall not access, transmit, receive, create, or distribute content that is prohibited by law, this policy, or other School policies.
3. Users shall not use the School's systems for unlawful purposes, including hacking, unauthorized access, circumvention of security measures, vandalism, introduction of malware, or interference with the operation of the School's network or devices.
4. Users shall not engage in cyberbullying, harassment, threats, discrimination, stalking, obscene conduct, or other inappropriate behavior using the School's network, devices, or online services.
5. Users shall not use the School's systems for unauthorized personal commercial activity, personal financial gain, or private business purposes.
6. Users shall not install unauthorized software, applications, extensions, or programs on School-owned devices or systems.
7. Users shall immediately report any security concern, suspected malware, accidental access to prohibited content, or unauthorized disclosure of information to a teacher, supervisor, or the Principal, as appropriate.

VI. Student Use and Monitoring.

Students may use School technology and internet resources only as authorized by School personnel and for educational purposes. Student use of internet-enabled devices and online resources shall be supervised by instructional or administrative staff as appropriate to the student's age and the activity involved. The School shall monitor the online activities of minors to the extent practical through a combination of staff supervision, network oversight, administrative review, and technological tools. Staff members responsible for supervising students shall make reasonable efforts to monitor student use to ensure compliance with this policy and applicable law.

VII. Education of Minors Regarding Appropriate Online Behavior.

The School shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction may be provided through classroom instruction, digital citizenship programming, student orientation, handbook review, or other School-directed means. This instruction shall include, as appropriate:

1. safe and responsible use of the internet;
2. appropriate behavior on social networking websites, in chat rooms, in email, and in other forms of direct electronic communication;
3. cyberbullying awareness and response;
4. protection of personal information and privacy online; and
5. compliance with School rules governing use of technology and internet resources.

VIII. Social Media, Messaging Platforms, and Online Communications.

Students may use only School-approved or School-authorized email, messaging platforms, chat functions, and online collaboration tools, and only when permitted by School personnel for educational purposes. Students shall not use the School's network or devices to communicate with unknown individuals or to participate in unauthorized social networking, messaging, or chat activity. Students are prohibited from accessing social media platforms, except when expressly directed by a teacher for an educational purpose. Prior to requiring students to use online content, staff shall confirm that the content is not blocked by the student internet filter. Staff may request that blocked content or social media platforms be reviewed and unblocked for educational purposes. TikTok, and any successor platforms, are prohibited on all School-owned devices and on any device, including a privately owned device, connected to School-provided internet. TikTok, and any successor platforms, may not be used to communicate or promote the School, any School-sponsored club, extracurricular organization, or athletic team.

IX. Protection of Student Information.

The School shall make reasonable efforts to protect against the unauthorized disclosure, use, or dissemination of students' personal information through its selection of online services, implementation of security practices, administrative controls, and user training. Staff shall not require students to use websites, web or mobile applications, software, or online services that do not protect against the disclosure, use, or dissemination of students' personal information in accordance with applicable law and the School's requirements.

X. School Administrative Responsibilities.

School administration shall be responsible for implementing this policy and may establish procedures, practices, or administrative rules consistent with this policy. Such responsibilities include:

1. implementing and maintaining the School's technology protection measure;
2. monitoring network use and online activity to the extent practical;
3. restricting or revoking user access when necessary to protect students, staff, or the security of School systems;

4. reviewing requests to unblock or permit access to blocked content or social media platforms for legitimate educational or administrative purposes;
5. providing or coordinating training for staff and age-appropriate instruction for students;
6. maintaining reasonable documentation regarding policy adoption, annual review, implementation, and compliance; and
7. implementing and enforcing the School's prohibition on TikTok and any successor platforms on School-owned devices and on any device, including a privately owned device, connected to School-provided internet, and prohibiting the use of TikTok or any successor platforms to communicate or promote the School, any School-sponsored club, extracurricular organization, or athletic team.

XI. Violations and Consequences.

Any violation of this policy may result in suspension or revocation of access privileges, confiscation of School-issued devices where appropriate, disciplinary action under the Code of Student Conduct or personnel policies, and referral to law enforcement when warranted. Students and employees are expected to cooperate in investigations of suspected misuse of School technology or internet resources.

XII. No Expectation of Privacy.

Users of School-owned devices, School networks, and School-provided internet access should have no expectation of privacy in their use of such systems, except as otherwise provided by law. The School reserves the right, subject to applicable law, to monitor, access, review, log, or disclose network activity, communications, and data stored on or transmitted through School systems for educational, operational, safety, security, and compliance purposes.

XIII. Parental and Public Access.

A copy of this policy shall be made available through the School's website, handbook, or other customary means of publication so that parents and guardians are informed of the School's internet safety requirements and practices.

XIV. Board Adoption.

This Internet Safety Policy shall be reviewed and approved annually by the Governing Board by September 1 of each year. This Internet Safety Policy was adopted by the Governing Board of Newberry Community School at a duly noticed public meeting at which the Governing Board addressed the proposed Internet Safety Policy and the proposed technology protection measures.