

IDEA Florida, Inc. Board Policy
Internet Safety Policy

SEC. 1. PURPOSE OF POLICY.

The purpose of this policy is to establish internet safety policies adopted by the IDEA board.

Rulemaking Authority 1001.02(1), (2)(n), 1003.02(1)(g)5. FS. Law Implemented 1003.02(1)(g) FS.

- (a) By September 1 of each year, IDEA Florida must adopt an internet safety policy for student internet use that applies to all devices owned or provided by a district or school, or any device (including privately owned) connected to district- or school-provided internet. This policy must be reviewed and approved annually by the school board or governing board.
- (b) It is the policy of IDEA to:
1. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
 2. Prevent unauthorized access and other unlawful online activity;
 3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
 4. Comply with the Children’s Internet Protection Act (“CIPA”), the Neighborhood Children’s Internet Protection Act (“NCIPA”), and the Protecting Children in the 21st Century Act, to the extent such laws are applicable to IDEA.
- (c) It is the goal of this policy not only to prevent and protect, but also to educate employees, students, parents, and the IDEA community in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by IDEA into its Acceptable Use Policy and/or Acceptable Use Agreement(s). All limitations and penalties set forth in the Acceptable Use Policy and/or Acceptable Use Agreement(s) 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. COMPLIANCE WITH THE REQUIREMENTS OF CIPA

a. 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. IDEA utilizes a sophisticated content filtering system that is compliant with CIPA and NCIPA on all computers that access the Internet.

- *As defined by CIPA, the term “technology protection measure” means a specific technology that blocks or filters Internet access to visual depictions that are:
- a. Obscene, as that term is defined in section 1460 of title 18, United States Code;
 - b. Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or
 - c. Harmful to minors.

The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

IDEA Florida, Inc. Board Policy Internet Safety Policy

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.

The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

b) 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, minimized only for bona fide research or other lawful purposes.

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

c) Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of IDEA’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:

1. Unauthorized access, including so-called “hacking” and other unlawful activities; and
2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

d) Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) to supervise and monitor usage of IDEA’s computers, computer IDEA 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 each Principal or designee.

e) Education

IDEA will advocate and educate employees, students, parents and IDEA community on Internet safety and “cyber-bullying.” Education will be provided through such means as professional

IDEA Florida, Inc. Board Policy Internet Safety Policy

development training and materials to employees, PTO/PTA presentations, and the IDEA website.

Additionally, the Principal or designee will provide age-appropriate training for students who use IDEA's Internet facilities. The training provided will be designed to promote IDEA's commitment to:

1. The standards and acceptable use of Internet services as set forth in the Acceptable Use Policies.
2. Student safety with regard to:
 - a. safety on the Internet;
 - b. appropriate behavior while online, on social networking websites, and in chat rooms; and
 - c. cyberbullying awareness and response.
3. Compliance with the E-rate requirements of CIPA.

Following receipt of this training, the student will acknowledge that he/she has received the training, understood it, and will follow the provisions of the Acceptable Use Policy and/or Acceptable Use Agreement(s).

f) Cyberbullying

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

IDEA is a place of tolerance and good manners. Students may not use the network or any IDEA 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, IDEA computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Ohio, or local laws. This includes, but is not limited to, any threat or act of intimidation or harassment against another person.

SEC 2. INTERNET SAFETY.

- (a) In developing a student internet safety policy, district school boards and governing boards must review whether the Children's Internet Protection Act, 47 C.F.R. § 54.520, applies and, if so, ensure compliance with CIPA.
- (b) Student internet safety policies must, at a minimum:
 1. Require the use of 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 at each school;

IDEA Florida, Inc. Board Policy
Internet Safety Policy

2. Protect the safety and security of students when using email, chat rooms, and other forms of direct electronic communications;
 3. Require the use of technology protection measures to prevent hacking or unauthorized access by students to data or information that they should not have access to, and to prohibit other unlawful online activities by students;
 4. Prevents access to websites, web or mobile applications, or software that do not protect against the disclosure, use, or dissemination of students' personal information in accordance with rule 6A-1.0955, F.A.C.; and
 5. Prohibits students from accessing social media platforms, except when expressly directed by a teacher for an educational purpose.
- (c) Prior to requiring students to use online content, policies must require staff to confirm the content is not blocked by the student internet filter. Policies must provide a process for staff to request that blocked content or social media platforms to be reviewed and unblocked for educational purposes.

1003.02(1)(g)

SEC. 3. TIKTOK.

In accordance with Florida state law, the IDEA board:

- (a) Prohibits the use of TikTok, and any successor platforms, on all district- or school-owned devices, or on any device (including privately owned) connected to district- or school-provided internet; and
- (b) Prohibits the use of TikTok, or any successor platforms, to be used to communicate or promote any school district, school, school-sponsored club, extracurricular organization, or athletic team.

1003.02(1)(g)5

SEC. 4. TRAINING AND UPDATES.

IDEA shall properly train or ensure training is provided to IDEA officers and employees on the requirements of this policy and any administrative procedures adopted to implement this policy. Additionally, IDEA shall notify IDEA officers and employees of any changes to this policy and related requirements.

SEC. 5. ADMINISTRATIVE PROCEDURES.

IDEA shall formally adopt administrative procedures as reasonably necessary to properly administer this policy and to adhere to applicable law and rule. In doing so, IDEA shall not adopt, and are prohibited from adopting, an administrative procedure that conflicts with applicable law or this policy. Accordingly, IDEA shall confer with the Board or legal counsel before deviating from the requirements set forth in this policy. In the event that a deviation from this policy becomes necessary, IDEA shall either recommend an amendment to this policy or the Board's approval of a specific deviation, including the purpose, scope and duration of the requested deviation.

SEC. 6. DATE ADOPTED AND EFFECTIVE.

**IDEA Florida, Inc. Board Policy
Internet Safety Policy**

As set forth in the pertinent minutes to the meeting of the Board, the Board amended this policy on June 26, 2024, and it became effective on June 26, 2024.

SEC. 7. RETENTION.

This policy shall be retained until superseded, expired, or discontinued and for five (5) years thereafter in accordance with state law.

SEC. 8. CERTIFICATION.

The Undersigned, being the Secretary of the Corporation, hereby certifies that the foregoing represents a true copy of the Board Policy relating to the Florida Internet Safety Policy as originally adopted by the Board on June 26, 2024, which Policy, as amended, is in full force and effect and has not been revoked or amended

DocuSigned by:
Christina Barker

6D9D79D477BD4C1...
Christina Barker, Board Chair

8/1/2024

Date Certified