INTERNET SAFETY 3.43*+

Introduction

I. It is the policy of the Sarasota County School District, utilizing the available resources and to the greatest extent possible, 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 [Pub. L. No. 106-554 and 47 USC 254(h)].

D. Implement technology protection measures that will:

1. filter or block access to material that is not appropriate for students based upon the subject matter and/or the age of the students served at each school;
2. prevent hacking or unauthorized access by students to data or information that they should not have access to, or other unlawful online activities by students;
3. prevent 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 Florida Administrative rules; and
4. prohibit students from accessing social media platforms, except when expressly directed by a teacher for an educational purpose

E. Utilizing the available resources, and to the extent practical, protect the safety and security of students when using email, chat rooms, and other forms of direct electronic communications

II. Access to Inappropriate Material

A. 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;

Formatted: Not Highlight

Formatted: Not Highlight

B. Protect the safety and security of students when using email, chat rooms, and other forms of direct electronic communications;

C. 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;

D. 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

E. Prohibits students from accessing social media platforms, except when expressly directed by a teacher for an educational purpose.

F. TikTok. School districts and charter school governing boards must:
   1. Prohibit 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
   2. Prohibit 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.
   3. Prohibit the use of any additional application or platform on the prohibited list as stated by the Florida Department of Management Services.

G. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter the Internet, or other forms of electronic communications, access to inappropriate information.

H. 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.

I. 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.

III. Inappropriate Network Usage

A. To the extent practical, steps shall be taken to promote the safety and security of users of the Sarasota County School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
B. Specifically, as required by the Children's Internet Protection Act, 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.

IV. Education, Supervision and Monitoring

A. It shall be the responsibility of all members of the Sarasota County School District 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. Prior to requiring students to use online content, staff must 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.

C. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the IT Department or designated representatives.

Formatted: Not Highlight

D. Each Sarasota County School shall provide age-appropriate training for students who use the District's Internet facilities. The training provided will be designed to promote the District's commitment to:

Formatted: Not Highlight

1. The standards and acceptable use of Internet services as set forth in the School District's Internet Safety Policy;
2. Student safety with regard to:
   a. safety on the Internet;
   b. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
   c. cyberbullying awareness and response.

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

V. Adoption

A. Internet Safety. The following policy guidelines are in place to protect students and visitors:

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
   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.

2. Prevent unauthorized access and other unlawful online activity
   a. To the extent practical, steps shall be taken to promote the safety and security of users of the online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
   b. Specifically, as required by the Children's Internet Protection Act, 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

3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors.

4. Provide student education, supervision and monitoring
   a. School staff will 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 IT Department.
c. Schools will provide age-appropriate training for students who use the Internet facilities.
d. The training provided will be designed to promote the commitment to:
    1. The standards and acceptable use of Internet services as set forth in the AUP and Internet Safety Policy guidelines.

    2. Student safety with regard to:
    (a) Safety on the Internet.
    (b) Appropriate behavior while on online, on social networking Web sites, and in chat rooms.
    (c) Cyberbullying awareness and response.

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

    4. 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 and Internet Safety policy guidelines.

    5. Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

B. Acceptable Use of the Digital Network of the Sarasota County School District The following are typical uses of the digital network:

1. Students' use of the District's digital network, internet service and other electronic resources is a privilege. As a condition of that privilege, students must comply with this Acceptable Use Policy ("AUP").

2. The following general rules govern students' use of the District's digital network and technology resources:
    a. The use must be in support with the District's educational goals and policies.
    b. The use must comply with this Acceptable Use Policy ("AUP").

c. The use must comply with the instructions of teachers and staff.

3. Require that students who access our network with district or personally owned electronic equipment ANNUALLY sign this Acceptable Use Agreement which is to be kept on file at each school or district department.

4. The use must comply with applicable laws and regulations, Including
   a. bullying and harassment and
   b. copyright laws.

VI. Prohibited Activities

A. The following are prohibited:
   1. Use that violates the Code of Conduct.
   2. Use of another individual's account or providing individual account information to another person.
   3. Use of the network for financial gain or for political or commercial activity.

B. Attempting to send or sending anonymous messages of any kind or pretending to be someone else while sending a message.

C. Attempting to access, modify, harm or destroy another user's data on the network.

D. Harassing, insulting, ridiculing, attacking or defaming others via network communications.

E. Attempting to subvert, defeat or disable installed web or network access filters, workstation security software, antivirus software or other features, network firewalls or other measures in place to secure the school district's technology resources.

F. Users of unauthorized methods of access to Sarasota County School District technology resources such as modems and virtual private networks (VPN's).

G. Use of remote access software or services to access remote computer networks, workstations or servers from the district system.

H. Attempting to transmit damaging agents (e.g., computer viruses,

Trojan horses, worms) or otherwise willfully damaging or disrupting any computer facility, software, or data.

I. Attempting to interfere with the normal operation of computers, terminals, peripherals, or networks.

J. Usage invades the privacy of others.

K. Use or experimentation with software or hardware without written approval from the CIO. • Willfully publishing, storing, displaying, transmitting, playing, or editing material that is obscene, threatening, profane, prurient, sexually suggestive or otherwise inappropriate.

L. Changing, deleting or modifying Internet browser settings including hiding or deleting Internet history or records of Internet use.

M. Use of the system for an unauthorized purpose.

N. Broadcasting a WiFi signal or operating a personal Hotspots from personal devices.

O. Students shall not perform any kind of maintenance, repair, configuration or installation services on District owned devices.

VII. Enforcement

Students who violate these procedures may be denied access to Sarasota County School District computing or technology resources and may be subject to disciplinary action, including possible expulsion. Alleged violations will be subject to the Sarasota County School District disciplinary procedures.

VIII. No Expectation of Privacy

Students and visitors have no expectation of privacy in their use of the District system.

IX. AUP Agreement and Acknowledgement

As a condition of the privilege of using the District's system and technology resources, students/parents are required to annually acknowledge and agree to the District AUP guidelines contained herein via the District's online Returning Student Verification form or the online New Student Enrollment form. AUP acknowledgement via the District's online forms (noted above) is the primary method recommended because that process also updates our student information

system. The AUP form found in this document is included for illustration and can be used (if needed).

X. The Use and Operation of Personally Owned Technology Devices or Electronic Property Students and visitors who are authorized to use or operate personally owned devices must adhere to the following:

A. District employees are not authorized to install software, perform any repair, configuration or maintenance on student-owned technology resources, that are brought to school property or present during school sponsored activities including both software and hardware resources.

B. Students who are authorized to bring and/or use a personally owned technology devices are responsible for the safe keeping and proper use of their property. The District is in no way liable for any loss or damage for student-owned devices.

C. Schools/Departments will not be responsible to hold or store student-owned devices.

XI. Additional Requirements

A. Students or Visitors Requesting a Waiver for Personal Electronic Property or Bring Your Own Device (BYOD)

B. Students and visitors requesting to operate their personal computing device (notebook computer, touch tablet, etc.) within the district must obtain written approval and abide by the following additional requirements: Any computer that is connected to the District Digital Network via wired or wireless control must have functioning anti-virus software running with up-to-date virus definitions. ~~Preferable antivirus software includes those by Norton/Symantec, McAfee, and Trend Micro.~~ A Waiver for Personal Electronic Property form must be signed (denoting approval) by the school or district department administrator prior to operating any personal electronic property in Sarasota County School District schools or offices. Any student or visitor that operates any personal electronic property must also sign and acknowledge this AUP.

C. Additional Guidelines for Students Student users must adhere to the following additional guidelines:
1. Students will follow teacher instructions regarding the use of the Sarasota County digital network.
2. Students must observe and adhere to all regulations when

using any digital device on school campus or during sponsored events including cell phone use as outlined in the Student Conduct Code.

D. Additional Rules Governing the Use of Video, Photo and/or Audio Recording Devices at School This section addresses the use of devices that can record audio, photo or video content in the school environment, particularly the classroom. ~~Such recording devices include:~~

~~1. Smart Pen (i.e. Livescribe Echo), Personal audio recorder~~
~~2. Mobile/Smart Phone (i.e. iPhone), Personal Media Player/MP3/MiniDisc Player (i.e. iPod)~~
~~3. Mobile Tablet or Slate Device (i.e. iPad, Nexus), eReader (i.e. Nook, Kindle)~~
~~4. Mobile Computer System capable of recording video, photo, audio (i.e. notebook, netbook)~~
~~5. Digital or film-based Camera or video recorder~~
~~6. Digital or film-based Audio Recorder (i.e. Cassette player)~~

E. Except at open house and public events as discussed below, students, parents and visitors are not allowed to videotape, photograph or make audio recordings while on school premises. All recording devices must be turned off at school. Staff shall only videotape, photograph or make audio recordings of students in furtherance of an educational objective. Except at open house and public events no such images of students shall be broadcast, posted, released, or otherwise disclosed by District staff without first obtaining parental consent.

F. Open House and Public Events Exception. Open house and public events are events where school premises are opened to the public or a segment of the public at the direction of the principal. They include: open houses, sporting events, plays, musicals, contests, fairs, fund raisers, awards/recognitions and theatre performances. They also include off campus events such as graduations, contests, fund raisers and other school sponsored public events. In the exercise of judgment and discretion, a principal may also allow videotaping or photographing under other circumstances, provided that appropriate steps are taken to prevent unwarranted disclosure of student images contrary to their directory information optout election and to avoid disruption of the educational environment.

XI. Exclusions

A. Students and staff using AI software with a personal device and/or personal credentials should be aware that the platforms they are

Formatted: Normal, Indent: Left: 0.94", No bullets or numbering

Formatted: Normal, Indent: Left: 0.94"

Formatted: Normal, Indent: Left: 0.94", No bullets or numbering

Formatted: Normal, Indent: Left: 0.94"

Formatted: Normal, Indent: Left: 0.94", No bullets or numbering

Formatted: Normal, Indent: Left: 0.94"

Formatted: Normal, Indent: Left: 0.94", No bullets or numbering

Formatted: Normal, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

uploading information to is collecting various forms of data and their privacy may not be protected.

~~F.~~A. ___

Formatted: Right: 0", Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75", Tab stops: Not at 1"

STATUTORY AUTHORITY: **1001.41, 1001.42, F.S.**

LAW(S) IMPLEMENTED: **1001.02, 1003.02 F.S.**
Rule 6A-1.0957, 6A-1.0955

HISTORY: **ADOPTED: _____**
REVISION DATE(S): _____