Office of Superintendent of Schools
Board Meeting of July 23, 2025

July 9, 2025

Office of the General Counsel
Walter J. Harvey, General Counsel

SUBJECT: **<u>INITIAL</u> READING: PROPOSED AMENDMENTS TO SCHOOL BOARD POLICIES 5500, *STUDENT CONDUCT AND DISCIPLINE* (*ELEMENTARY/SECONDARY CODE OF STUDENT CONDUCT*), 7540, *COMPUTER TECHNOLOGY AND NETWORKS*, AND 7540.03, *STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS & INTERNET SAFETY***

COMMITTEE: **PERSONNEL, STUDENT, SCHOOL & COMMUNITY SUPPORT**

LINK TO STRATEGIC PLAN: **SAFE, HEALTHY & SUPPORTIVE LEARNING ENVIRONMENTS**

Consistent with the Board's responsibility to review and amend policies to conform to legislative changes and updates to District practices, authorization is requested for the Superintendent to initiate rulemaking proceedings to amend School Board Policies 5500, *Student Conduct and Discipline* (Elementary and Secondary Codes of Student Conduct), 7540, *Computer Technology and Networks*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety.* These policies are proposed for amendment to incorporate the requirements of 2025 Florida House Bill 1105 ("H.B. 1105") and House Bill 1255 ("H.B. 1255") that became effective July 1, 2025, and to reflect current District practices.

Policy 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, and the Elementary and Secondary Codes of Student Conduct ("COSC") incorporated by reference in Policy 5500, *Student Conduct and Discipline*, are proposed for amendment in response to H.B. 1105. Pursuant to H.B. 1105, Policy 7540.03 and each COSC would be revised to provide that students in grades K–8 are prohibited from using wireless communication devices ("WCDs") during the school day, except for in designated areas with administrative approval or when authorized by a disability accommodation plan or by a doctor for medical reasons. High school students, meanwhile, may use WCDs during the school day, but remain prohibited from using WCDs during instructional time unless directed to do so by a teacher solely for educational purposes. Additionally, to account for a pilot program created by H.B. 1105 which would prohibit WCD use in all grades, these provisions are made subject to State Board of Education and Florida Department of Education rules and directives. Policy 7540, *Computer Technology and Networks*, is also proposed for amendment to clarify that WCDs, as defined in that policy, are separate from the "instructional mobile devices" that the District either issues to students or allows them to bring solely for instruction under the District's bring-your-own-device program.

Pursuant to H.B. 1255, each COSC is additionally proposed for amendment to provide that if a student's disobedient, disrespectful, violent, abusive, uncontrollable, or disruptive behavior continues, the school principal will refer the case to the Student Support Team to schedule a meeting with the parent, identify potential remedies, and take additional steps allowed or required by law. Each COSC would also provide that expulsions for zero-tolerance offenses may be extended based on a threat

management team's determination. Each COSC is otherwise proposed for amendment to incorporate prohibitions on trespassing on school buses and cheating on standardized tests, to clarify existing offenses and prohibitions, and to provide that required notices can be issued to parents in a manner they agree to in writing.

These policy amendments were drafted in collaboration with and reviewed by the Superintendent, Cabinet, and District staff. The Notice of Intended Action and policies with strikethroughs and underlines are attached.

The proposed revisions to each COSC can be accessed by visiting the following links:

- Elementary Code of Student Conduct
- Secondary Code of Student Conduct

RECOMMENDED: That The School Board of Miami-Dade County, Florida, authorize the Superintendent to initiate rulemaking proceedings in accordance with the Administrative Procedure Act to amend School Board Policies 5500, *Student Conduct and Discipline*, 7540, *Computer Technology and Networks*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety.*

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on July 23, 2025, its intention to amend School Board Policies 5500, *Student Conduct and Discipline*, 7540, *Computer Technology and Networks*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, at its meeting of September 10, 2025.

PURPOSE AND EFFECT: Policies 5500, *Student Conduct and Discipline*, 7540, *Computer Technology and Networks*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, are proposed for amendment in response to 2025 Florida House Bill 1105 ("H.B. 1105") and House Bill 1255 ("H.B. 1255"), updates to District practices, and to clarify current provisions.

SUMMARY: Pursuant to H.B. 1105, Policy 7540.03 and each Code of Student Conduct (COSC) would be revised to provide that students in grades K–8 are prohibited from using wireless communication devices ("WCDs") during the school day unless an exception applies, while high school students may use WCDs during the school day, but remain prohibited from using WCDs during instructional time unless directed to do so for educational purposes. To account for a new pilot program, these provisions are made subject to state-issued directives. Policy 7540 is also proposed for amendment to clarify that WCDs are separate from "instructional mobile devices." Pursuant to H.B. 1255, each COSC is also proposed for amendment to provide that if a student's misbehavior continues, a school principal will refer the case to the Student Support Team to schedule a meeting with the parent, identify potential remedies, and take additional steps required or allowed by law. Each COSC would also provide that expulsions for zero-tolerance offenses may be extended. Each COSC is otherwise being amended to incorporate prohibitions on trespassing on school buses and cheating on standardized tests, to clarify existing offenses and prohibitions, and to provide that required notices can be issued to parents in a manner they agree to in writing.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: Fla. Stat. ss. 1001.41(1)–(2), 1001.42(8), 1001.43(1), 1001.51(24), 1006.07(1); Fla. Admin. Code r. 6A-1.0957

LAWS IMPLEMENTED INTERPRETED OR MADE SPECIFIC: Fla. Stat. ss. 810.097, 1006.07, 1006.09, 1006.15, 1006.165, 1006.13; Fla. Admin. Code r. 6A-1.0017, 6A-1.0957.

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF September 10, 2025, which begins at 1:00 p.m., in the School Board Auditorium, 1450 N.E. Second Avenue, Miami, Florida 33132. Persons requesting such a hearing or who wish to provide information regarding the statement of estimated regulatory costs, or to provide a proposal for a lower cost regulatory alternative as provided in Section 120.54(1), F.S., must do so in writing by August 19, 2025, to the Superintendent, Room 912, at the same address.

ANY PERSON WHO DECIDES TO APPEAL THE DECISION made by the School Board of Miami-Dade County, Florida, with respect to this action will need to ensure the preparation of a verbatim record of the proceedings, including the testimony and evidence upon which the appeal is to be based. (Section 286.0105, Florida Statutes)

COPIES OF THE PROPOSED AMENDED POLICIES are available at cost to the public for inspection and copying in the Citizen Information Center, Room 158, 1450 N.E. Second Avenue, Miami, Florida 33132.

Book	Policy Manual
Section	July 23, 2025 - Initial Reading
Title	**STUDENT CONDUCT AND DISCIPLINE**
Code	5500
Status	Initial Reading

5500 - **STUDENT CONDUCT AND DISCIPLINE**

Schools shall promote a positive school climate that supports academic achievement and emphasizes civility, fairness, mutual respect, and acceptance of diversity. The *Code of Student Conduct Elementary*, *Code of Student Conduct Secondary*, and the *Post-Secondary Code of Student Conduct*, incorporated by reference, apply to all students in the District. Copies of these documents are on file in the Office of Board Recording Secretary, and the Citizen Information Center, and shall be available in each school and special center.

The Superintendent, principals, and other administrators shall assign discipline/corrective strategies to students pursuant to the Code of Student Conduct and, where required by law, protect the student's due process rights to notice, hearing, and appeal. Additional guidelines for the maintenance of appropriate student behavior are issued by memorandum from District administration.

The Superintendent shall make the Code of Student Conduct available to all students and their parents.

See also Elementary Code of Student Conduct (Español and Kreyòl) and Secondary Code of Student Conduct (Español and Kreyòl).

To see the applicable code of student conduct in the appropriate language, please click here.

Effective 07.01.2011
Revised 01.16.2013
Revised 06.18.2014
Revised 04.15.2015
Revised 10.21.2020
Revised 01.18.2023

Revised 09.11.2024

Legal References:
F.S. 39.201, 39.201(2)(a), 39.301(16), 39.401, 39.401(1)(a), 119.07(1)(3)(h)
F.S. 120, 322.091, 394.463, 394.495, 561.01(4), 741.24, 775.082, 775.083
F.S. 775.084, 775.21, 790.001(13), 790.115, 790.161, 790.162, 790.163
F.S. 794.011, 794.024, 794.03, 806.13(2), 810.097, 827.03, 827.04, 827.071
F.S. 831.31, 836.10, 893, 893.02, 893.03, 893.13, 901.15(3), 921.0022
F.S. 943.0435, 985.04(7), 985.101, 985.481, 985.557, 1000.04, 1001.31
F.S. 1001.42, 1001.42(6), 1001.43, 1001.43(1)(6), 1002.20, 1003.01
F.S. 1003.02(1)(c)(2), 1003.04, 1003.31, 1003.32(e)(2)(3)(4)(5)(6)(a)(b)
F.S. 1003.53, 1006.04, 1006.07, 1006.08, 1006.09. 1000.05, 1006.10, 1006.12
F.S. 1006.13, 1006.135, 1006.147
F.A.C. 6A-1.0017
F.A.C. 6A-19.008
34 C.F.R. Part 106

Adoption Date: 05.11.2011

Book	Policy Manual
Section	July 23, 2025 - Initial Reading
Title	COMPUTER TECHNOLOGY AND NETWORKS
Code	7540
Status	Initial Reading

7540 - **COMPUTER TECHNOLOGY AND NETWORKS**

The School Board is committed to the effective, safe, and secure use of technology to provide for quality student learning, flexibility for employees to accomplish job tasks, and efficient Board operations. Safeguards shall be established so that the Board's investment in both hardware and software is achieving the benefits of technology and inhibiting negative side effects. The use of these technology resources is a privilege, not a right.

I. **Definitions**

The following definitions apply to this policy, Policy 5500, Policy 7530.01, and Policies ~~y~~ 7540.01 – ~~Policy~~ 7540.07:

A. "Artificial intelligence" is defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

B. "Deepfake" means audio or visual content that has been generated or manipulated by artificial intelligence which would falsely appear to be authentic or truthful and which features depictions of people appearing to say or do things they did not say or do without their consent.

C. "Digital applications/services" are a collective set of software programs, web-based platforms, and online tools used to carry out operations, communications, and educational functions in a digital environment. This includes, but is not limited to, all software,

websites, online applications, and digital tools owned, managed, or contracted by the District.

D. "District network" is defined as the underlying communication fabric that allows devices to interact with the Internet and each other. This includes network circuits, services, and resources such as routers, switches, firewalls, and wireless access points that enable the connection of District technology and networked devices to other computers, whether they are within the District or external to the District, including connection to the Internet.

E. "District technology" encompasses the District network and all connected systems and devices owned and managed by the District, including computer hardware, software, electronic mail systems, networked devices, cloud storage/solutions, and third-party solutions managed by the District and/or for which the District has contracted for services.

F. "Inappropriate use" means any use of the District network or District technology that is inconsistent with the goals, objectives, policies, and educational mission of the District (see Policy 7540.02).

G. "Instructional mobile devices" are defined as portable electronic computer equipment that can connect to the Internet, including but not limited to, tablets, laptops, e-readers, and other small form portable computing devices, that are used for teaching and learning. This term includes personal devices authorized to be used solely for educational purposes under the District's bring-your-own-device program (Policy 7540.01).

H. "Legitimate District purposes" are those actions directly promoting the educational, instructional, administrative, business, and support services missions of the District and that are related to any instruction, project, job, work assignment, task, or function for which the user is responsible.

I. "Obscene material" means material that: (a) the average person, applying contemporary community standards, would find, taken as a whole, appeals solely to the prurient interest; (b) depicts or describes, in a patently offensive way, sexual conduct as defined in State law (F.S. 847.001(11)); and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value.

J. "Personal devices" are non-District owned devices, including personally-owned wireless communication devices, that are capable of processing, storing, or transmitting information.

K. "Phishing" is a fraudulent attempt to obtain sensitive information or data such as usernames, passwords and credit card details, or to install malicious software, by disguising oneself as a trustworthy entity in an electronic communication.

L. "Social media" is defined as forms of electronic communication through which users create online communities or groups to share information, ideas, personal messages, and other content.

M. "Spamming" means to send unwanted, unsolicited, and/or unnecessary messages to large numbers of people, usually with the purpose of advertising a product, event, service, or lobbying for a specific political position, or promoting an individual's opinion.

N. "Spoofing" is the act of disguising the sender of a message by replacing the name in the "from" or header fields, sending messages while signed on as a different user, or otherwise intentionally misleading the recipient as to the identity of the actual sender.

O. "Staff members" are all District employees, consultants, vendors, auditors, temporary help, volunteers, and others authorized by the District to access the District network for the performance of their job duties, responsibilities, or functions.

P. "User" is defined as anyone accessing the District network, including but not limited to students and staff members.

Q. "Wireless communication devices" are any ~~handheld~~ devices used or capable of being used in a handheld manner (including but not limited to ~~a~~ cellphones, ~~a~~ tablets, ~~a~~ laptops, smartwatches, smartglasses, or ~~a~~ two-way messaging devices) that are designed or intended to receive or transmit text or character-based messages, access or store data, or connect to the Internet or any communications service. This term does not include instructional mobile devices.

II. Instruction, Training, and Development of Procedures

A. The Superintendent shall develop protocols, guidelines, and/or procedures for the proper acquisition of technology and to provide guidance to staff members, students, and other users about making safe, appropriate, and ethical use of computers and other equipment and networks that may be established in physical or virtual environments. These procedures shall also inform staff members and students about actions, including but not limited to disciplinary actions, that will be taken if District technology is abused in any way or used in an illegal or unethical manner or if unauthorized devices

are connected to the District network.

B. Students shall be educated about appropriate online behavior, including but not limited to instruction on social media, as required by F.S. 1003.42; interacting appropriately with other individuals online; and recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses to cyberbullying (see Policy 5500, *Student Conduct and Discipline*).

C. The Superintendent is authorized to develop procedures governing the use of artificial intelligence. Students and staff members will be informed of the District's requirements regarding the ethical, responsible, and safe use of artificial intelligence in accordance with District procedures and applicable state and federal laws, regulations, and Board policies. Inappropriate use of artificial intelligence is prohibited.

D. Staff members will be trained at least annually on cybersecurity, including but not limited to the identification of cyber threats and the appropriate procedures to follow when a threat is suspected.

Effective 07.01.2011
Revised 12.09.2020
Revised 07.24.2024

Legal References:
F.S. 1001.43

Adoption Date: 05.11.2011

Book	Policy Manual
Section	July 23, 2025 - Initial Reading
Title	STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS
Code	7540.03
Status	Initial Reading

7540.03 - **STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS**

The School Board provides students access to a large variety of technology and network resources which provide multiple opportunities to enhance learning and improve communication within the District and the community. All students must, however, exercise appropriate and responsible use of school and District technology and information systems. This policy is intended to promote the most effective, safe, productive, and instructionally sound uses of network information and communication tools.

I. **District Network Resources**

The Board shall maintain the District network, as defined in Policy 7540, and a system of internet content filtering devices and software controls that meet the standards established in the Children's Internet Protection Act (CIPA) and other applicable State and Federal laws and regulations.

II. **Internet Safety**

A. The District shall limit student access to the Internet:

1. to only materials that are appropriate for students, taking into consideration the subject matter and the age of the students served at each school;

2. in a manner that protects the safety and security of students when using e-mail, chat rooms, and other forms of direct

electronic communications;

3. in a manner that prohibits unauthorized access by students to data or information, including through hacking and other unlawful online activities;

4. in a manner that prevents access to websites, web applications, or software that does not protect against the disclosure, use, or dissemination of students' personal information;

5. in a manner that prohibits and prevents students from accessing social media platforms through the use of Internet access provided by the District, except when expressly directed by a teacher or appropriate staff solely for educational or school-related purposes;

6. in a manner that prohibits the use of the TikTok platform or any successor platform on District-owned devices, through Internet access provided by the District, or as a platform to communicate or promote any District school, school-sponsored club, extra-curricular organization, or athletic team.

B. Before requiring students to use online content for educational purposes, school personnel must confirm the content is not blocked by any student Internet filter. The principal may submit a request to the District's Information Technology Services (ITS) Department to have blocked content or social media platform reviewed and unblocked. Upon receipt of this request, ITS will review the blocked content for compliance with this policy and applicable cyber-security laws.

C. Any online educational service that students or their parents are required to use must comply with Policy 8330, *Student Information, Records, and Privacy Rights*, the "Student Online Personal Information Protection Act" (F.S. 1006.1494), and all relevant statutes and rules.

III. Digital Citizenship

The Board uses information and technology in safe, legal, and responsible ways, and expects students to behave as responsible digital citizens. A responsible digital citizen is one who:

A. Respects oneself:

Students will select online names that are appropriate and will consider the information and images they post online.

B. Respects others:

Students will refrain from using the District network and social media

to bully, tease, or harass other people.

C. Protects oneself and others:

Students will protect themselves and others by reporting abuse and not forwarding inappropriate materials or communications.

D. Respects authorship:

Students will properly reference or cite to work, websites, books, media, etc., used in any of their work.

E. Protects intellectual property:

Students will not use software and media produced by others without prior authorization from the owner, or upload, download, or transfer any intellectual property belonging to a third party (including images, texts, video files, and digital media files) without specific permission.

IV. Student Responsible Use

A. Responsible use of the District network is expected to be ethical, respectful, academically honest, and supportive of the District's mission. Each student has the responsibility to respect every other person in our community and on the Internet.

B. District technology will be treated as extensions of the physical school space. Administrators, their designees, or contracted entities may review files and communications on District technology and related systems (including, but not limited to, electronic mail, managed chat applications, and network or cloud storage) to ensure that students are using these systems in accordance with Board policy and administrative procedures and guidelines. Students have no expectation of privacy in files stored electronically on District technology and related systems, which may be subject to disclosure pursuant to Florida's Public Records laws.

C. Students shall comply with the following rules of network etiquette, including but not limited to:

1. Use of District technology, electronic devices, and social media must be consistent with the District's educational objectives, mission, and curriculum. All students accessing the District network are bound by the guidelines and stipulations set forth in the District Network Security Standards, which are posted on the District's website.

2. Any student who identifies a security problem on the District network must notify a system administrator and shall not disclose or demonstrate the problem to others.

3. Students shall not use other individuals' accounts or log in to the system as any other user; share their passwords with anyone, except as authorized by Board policy; engage in activities that would reveal anyone's password; or allow others to access a computer that the student is logged on to. Attempting to log in to the system as any other user is prohibited. Students are expected to act with due care in keeping their passwords private and secure.

4. Transmission of any material in violation of any local, Federal, and State laws is prohibited. This includes, but is not limited to, copyrighted materials; licensed material; and defamatory, threatening, bullying, discriminating, slanderous, offensive, harassing, cyberstalking, or obscene material (as defined in Policy 7540).

5. Use of District resources to access, process, or display proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.

6. The District network may not be used to send or receive messages that discriminate on any protected basis as delineated in Board policies prohibiting discrimination (see Policy 5517).

7. The use of profanity, vulgarities, or any other inappropriate language is prohibited.

8. Cyberbullying is prohibited at all times, on or off school grounds, whether using personal devices, District technology, the District network, social media, or other broadband connections of any kind (see Policies 5500 and 5517.01).

9. Creating a deepfake is prohibited unless authorized by a teacher or administrator for a legitimate District purpose.

10. Software, services, games, applications, video or audio files, or streaming media without educational value may not be installed, uploaded/downloaded, or utilized on District technology without prior authorization by a teacher or administrator.

11. The creation of digital applications/services using District technology must be done under the supervision of an instructional staff member. Content on student-created digital applications/services must comply with Board policies and District procedures (see Policy 7540.02).

12. Use of District resources for commercial activities, product advertisement, religious or political campaigning, lobbying, or

solicitation is prohibited.

13. Accessing unmanaged or non-sanctioned chat rooms or instant messaging using District technology is prohibited.

14. Bypassing the District's content filter without authorization is strictly prohibited.

15. Students may be held personally and financially responsible for malicious or intentional damage or interruptions to network service, software, data, user accounts, hardware, and/or any other unauthorized use.

16. Files stored on District technology are the property of the District and may be monitored or inspected by administrators, their designees, or contracted entities at any time.

17. Materials published electronically using District resources must be for educational purposes. Administrators may monitor these materials to ensure compliance with content standards.

V. Additional Requirements

A. Students shall receive education and/or information about the following:

1. safety and security while using e-mail, chat rooms, social media, and other forms of electronic communications;

2. the dangers inherent in online disclosure of personally identifiable information;

3. the consequences of prohibited acts (e.g., hacking, cyberbullying, and other unlawful or inappropriate activities online);

4. the social, emotional, and physical effects of social media and any related requirements, as set forth in F.S. 1003.42; and

5. the ethical, responsible, and safe use of artificial intelligence.

B. All students (and their parents if they are minors) are required to sign a written agreement annually, or at the time of enrollment, to abide by the terms and conditions of this policy and its administrative procedures and guidelines.

C. A student may possess a wireless communications device (WCD) while the student is on school property or in attendance at a school function~~;~~. H~~h~~owever, ~~a~~ students in grades K–8 may not use ~~a~~ WCDs during the school day, and students in grades 9–12 may not use WCDs during

instructional time, except when expressly directed by a teacher solely for educational purposes. Exceptions will be made only when:

1. school administrators have given express permission for students to display or use WCDs in designated locations within the school building(s); or

2. the display or use of a WCD is in accordance with a student's individualized education plan, Section 504 plan, or a doctor's note from a licensed physician under Florida law certifying in writing that the student requires the use of a WCD based upon valid clinical reasoning or evidence.

This paragraph is subject to State Board rules and/or Florida Department of Education directives. ~~If authorization has been specifically given by the school for use of a WCD within the District's educational mission, students may bring their own WCD. However, teachers shall have authority to designate an area for WCDs during instructional time.~~

D. When WCD use is not authorized during instructional time, a student must place the WCD in an area designated by the teacher.

~~C.~~E. The District/school is not responsible if a student's WCD or any other personal device is damaged, lost, or stolen. Students will be notified of any additional responsibilities for use of these devices.

~~D.~~F. Consistent with Board policies and procedures pertaining to publications, an image taken using a camera device may not be published, broadcast, or transmitted to any other person, by any means, without the knowledge and consent of each person appearing in that image who had a reasonable expectation of privacy at the time the image was recorded, or the person who owns the copyright of the material appearing in that image. Cameras on WCDs may not be used:

1. in any unethical or illegal manner;

2. to photograph another person who has a reasonable expectation of privacy without that person's knowledge and consent;

3. in a way that would violate copyright laws;

4. to harass, intimidate, or bully another person or to invade another person's privacy;

5. in any classroom without a teacher's or principal's permission; or

6. in any locker room, restroom, or any other place where other people have a reasonable expectation of privacy.

~~E.~~G. Students are prohibited from utilizing the data access capabilities of a WCD, Internet hotspot, or any other connection method that bypasses Internet content filtering and/or District security mechanisms to connect to Internet-based resources (including, but not limited to, social media) during instructional time, unless approved or directed by their teacher and/or other authorized staff member.

VI. Social Media

When using social media, students shall comply with the same responsible use rules outlined above for Internet and District network use. In addition, students will not represent or create the inference on any social media posting that they speak on behalf of the school, the District, the Board, or its members. Use of District technology for personal social media activities is prohibited. Students may be disciplined by the District for inappropriate social media behavior even if it occurs off school grounds.

VII. Violations and Sanctions

Inappropriate use (as defined in Policy 7540) and violations of this or any other Board policy may result in suspension of District network access and/or discipline in accordance with Policy 5500, *Student Conduct and Discipline* and the applicable Code of Student Conduct. Student access may be denied if the school, Regional Center, or District administrator determines that a student has used the Internet or District technology in an inappropriate or unacceptable manner. Students may also be subject to other legal action.

VIII. Board Liability

The Board is not responsible for, and shall not be liable, for:

A. damage resulting from unauthorized or inappropriate use of the District network or social media activity;

B. the accuracy, quality, or use of information obtained via the Internet;

C. any damages caused by a user's negligence or error, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions;

D. unfiltered content that may be viewed or downloaded on District technology that has been provided to individuals for use outside of District property;

E. issues or damage caused by the connection of personal devices to the District network or improper use of the District network or District technology; or

F. personal devices that are damaged, lost, or stolen.

IX. Administrative Procedures and Guidelines

The Superintendent, or designee, is authorized to develop, implement, and disseminate administrative procedures and user guidelines necessary to effectuate this policy.

X. Annual Review of Policy

By September 1st of each year, the Board shall review and, if necessary, approve any changes to this policy.

Effective 07.01.2011
Revised 07.18.2012
Revised 06.17.2015
Revised 03.15.2017
Revised 08.16.2023
Revised 12.20.2023
Revised 07.24.2024

Legal References:
F.S. 112.22
F.S. 748.048
F.S. Chapter 847, et seq.
F.S. 1001.43
F.S. 1001.51
F.S. 1003.02
F.S. 1003.32
F.S. 1003.42
F.S. 1006.07
F.S. 1006.1494
F.A.C. 6A-1.0955
F.A.C. 6A-1.0957
P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h),(1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
20 U.S.C. 6777, 9134 (2003)
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246

47 C.F.R. 54.500 - 54.509, 54.511, 54.513 - 54.520, 54.522 - 54.523

Adoption Date: 05.11.2011