Office of Superintendent of Schools
Board Meeting of November 15, 2023

November 1, 2023

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

SUBJECT: **<u>INITIAL</u> READING: PROPOSED AMENDMENTS TO SCHOOL BOARD POLICIES 7530.01, *STAFF USE OF WIRELESS COMMUNICATION DEVICES*, 7540.03, *STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS & INTERNET SAFETY*, AND 7540.04, *STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS***

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

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

Consistent with the Board's statutory responsibility to periodically review and update policies to conform to legislative changes and State Board of Education rulemaking, authorization is requested for the Superintendent to initiate rulemaking to amend Board Policies 7530.01, *Staff Use of Wireless Communication Devices*, 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, and 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*.

Policy 7530.01, *Staff Use of Wireless Communication Devices*, is proposed for amendment to incorporate the requirements of section 112.22, Florida Statutes, which requires that public employers restrict access to any prohibited application on a government-issued device; prohibit such applications from being downloaded; and have procedures in place to remotely wipe and uninstall any prohibited application from a government-issued device that is believed to have been adversely impacted, either intentionally or unintentionally, by a prohibited application. A list of prohibited applications will be compiled and published by the Department of Management Services ("DMS") in the Florida Administrative Registrar, and a waiver of these prohibitions can be requested from the DMS under certain circumstances. Policy 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, is also proposed for amendment to incorporate this prohibition on downloading unauthorized applications.

Policy 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, is proposed for amendment as a result of State Board of Education Rule 6A-1.0957, "Internet Safety Policy" (Aug. 22, 2023). Rule 6A-1.0957 provides that before requiring students to use online content, staff to confirm the content is not blocked by the District's student internet filter. If the content is blocked, then there must be a process for staff

to request that it be reviewed and unblocked for educational use. The rule additionally provides that the Board's policy on internet safety be reviewed and approved annually. Policy 7540.03 is accordingly proposed for amendment to incorporate these requirements.

These policy amendments were drafted in collaboration with, and reviewed by, the Superintendent, Cabinet, and District staff.

The Notice of Intended Action and proposed policies with strikethroughs and underlines are attached.

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 Board Policies 7530.01, *Staff Use of Wireless Communication Devices*, 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, and 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*.

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on November 15, 2023, its intention to amend Board Policies 7530.01, *Staff Use of Wireless Communication Devices*, 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Systems & Internet Safety*, and 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, at its meeting of December 20, 2023.

PURPOSE AND EFFECT: Board Policies 7530.01, *Staff Use of Wireless Communication Devices*, and 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, are proposed for amendment to incorporate the requirements of F.S. 112.22. Board Policy 7540.03 is proposed for amendment to incorporate the requirements of F.A.C. 6A-1.0957.

SUMMARY: Board Policies 7530.01, *Staff Use of Wireless Communication Devices*, and 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, are proposed for amendment to incorporate the requirements of F.S. 112.22, which requires that public employers restrict access to any prohibited application on a government-issued device, prohibit such applications from being downloaded, and have procedures in place to remotely wipe and uninstall any prohibited application from a government-issued device that is believed to have been adversely impacted, either intentionally or unintentionally, by a prohibited application. Policy 7540.03 is additionally proposed for amendment as a result of F.A.C. 6A-1.0957 (Aug. 22, 2023), which requires staff to confirm that online content is not blocked by the District's student internet filter before requiring students to access that content. The rule additionally requires that the Board's internet safety policy be reviewed and approved annually.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: Fla. Stat. ss. 1001.32(2); 1001.41(1), (2); 1001.42(5), (6), (7), (8).

LAWS IMPLEMENTED INTERPRETED OR MADE SPECIFIC: Fla. Stat. ss. 112.02, 1003.02; Fla. Admin. Code r. 6A-1.0957.

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF December 20, 2023, 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 December 13, 2023, 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 POLICY 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	November 15, 2023- Initial Reading
Title	**STAFF USE OF WIRELESS COMMUNICATION DEVICES**
Code	7530.01
Status	Initial Reading

7530.01 - **STAFF USE OF WIRELESS COMMUNICATION DEVICES**

The School Board will provide wireless communication devices ("WCDs") (i.e. cellular and wireless telephones, pagers/beepers, personal digital assistants (PDAs) BlackBerries/Smartphones, WiFi-enabled or broadcast access devices, etc.) to employees who by the nature of their job have a routine and continuing business need for the use of such devices for official Board business. WCDs are provided as a tool to conduct Board business and to enhance business efficiencies. WCDs are not a personal benefit and shall not be a primary mode of communication, unless they are the most cost-effective means to conduct Board business (i.e. because some wireless services plan are billed on a time-used basis, Board-owned WCDs should not be used if a less costly alternative method of communication is safe, convenient and readily available).

The Superintendent is authorized to designate those staff members who will be issued a Board-owned WCD and provided with a wireless service plan.

The Superintendent is responsible for verifying:

A. the need for each Board-owned WCD and wireless service plan is clearly justified for Board business purposes;

B. alternative solutions for work production and communication are considered;

C. employees provided with wireless service plans are notified of the purpose and limitations of usage;

D. wireless service plan invoices outlining the details of usage are received and reviewed for conformance with this policy;

~~E.~~ employees reimburse the Board for non-business use; ~~and~~

E. ~~a Board-owned WCD is returned and the corresponding wireless service plan is terminated when it is no longer justified by business requirements, the employee leaves the Board's employment, and/or when the employee has demonstrated a disregard for the limitation of this policy.~~

F. that Board-owned WCDs are restricted from accessing any prohibited application as identified by the Florida Department of Management Services (DMS);

G. that the District retains the ability to remotely wipe and uninstall any prohibited application from the WCD that is believed to be have been adversely impacted, either intentionally or unintentionally, by a prohibited application; and

H. that a Board-owned WCD is returned and the corresponding wireless service plan is terminated when it is no longer justified by business requirements, the employee leaves the Board's employment, and/or when the employee has demonstrated a disregard for the limitation of this policy.

~~F.~~

In deciding which staff members should receive a Board-owned WCD, the Superintendent will consider whether their jobs:

A. require them to spend a considerable amount of time outside of their assigned office or work area during normal working hours and have regular access to telephone and/or Internet connections while outside their office or assigned work area;

B. require them to be accessible outside of scheduled or normal working hours or to be contracted and respond in the event of an emergency; ~~or~~

C. consistently require timely and business ~~-~~critical two (2) way communication for which there is not reasonable alternative technology~~; (This is not~~ (not intended to include occasional, incidental access or purely voluntary access such as checking e-mail from home~~.~~);

D. safety requirements indicate having a WCD is an integral part of meeting the requirements of the employee's job description;

E. more than fifty percent (50%) of the employee's work is conducted outside the employee's assigned office or work area;

F. the employee is required to be contacted on a regular basis outside normal work hours;

G. the employee is required to be on-call 24/7; or

H. the employee's job requirements include critical District-wide decision-making.

Board-owned WCDs and/or their related wireless service plan are to be used only to place calls, access the Internet, or receive/send e-mails, instant messages or text messages for District-related business. Board-owned WCDs are not to be used to place calls or send/receive e-mails, instant messages or text messages of a personal nature, or access the Internet for personal business.

Wireless service plans are expected to be set at the minimum level that fulfills the business need for the position in question. The wireless service plan that is selected for an employee should be the one that provides a combination of services including number of minutes, coverage, and local call zone most nearly matching the employee's recurring business needs as well as whether or not the service plan includes text messaging, instant message and/or e-mail capability, and ability to access the Internet. If the wireless plan is based on minutes used for calls made or includes a charge regarding e-mail or instant messages, the smallest plan available to accommodate the particular business need shall be utilized.

The Board shall approve the Superintendent's recommendation regarding the type and level of wireless service appropriate for each staff member listed above. In all cases, the Superintendent shall take the steps necessary to secure the most economical and responsible service available.

Thereafter, an annual review of the service plans available shall be made to determine if the District's wireless service plans are the most economical and responsible available. Additionally, at least once annually, the Superintendent shall review the employee's actual usage (i.e. type and level of service) with the employee and, if warranted, authorize the acquisition of a different WCD and/or selection of a different wireless service plan that more nearly matches the employee's recurring business needs. Any such change in provider and/or necessary adjustments to individual staff member's devices and/or service plans shall be presented to the Board for consideration and approval.

Possessing a Board-owned WCD is a privilege and all employees are expected to use them appropriately and responsibly. Employees are responsible for managing the cost effectiveness of WCD use by utilizing assigned landline and/or designated computers as available and appropriate. Employees should know that using a WCD to place calls outside the immediate area might result in roaming charges, in addition to long distance and regular charges, and that the Board is charged for both outgoing and incoming calls.

In order to continue to be eligible to receive a Board-owned WCD, staff members are required to answer all calls on ~~his/her~~their WCDs and promptly respond to any messages.

Employee safety is a priority of the Board, and responsible use of WCDs includes safe use.

Using a WCD while operating a vehicle is strongly discouraged. Employees should plan accordingly so that calls are placed, text messages, instant messages or e-mails sent/read, and/or the Internet browsed either prior to traveling or while on rest breaks. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws and Board policies while driving.

Confidentiality of Student Personally Identifiable Information; Public and Student Record Requirements

Employees are subject to all applicable policies and guidelines pertaining to protection of the security, integrity and availability of the data stored on their Board-owned WCDs.

Wireless communications, including calls, text messages, instant messages, and e-mails sent from WCDs may not be secure. Employees should use discretion in relaying confidential information related to students.

Additionally, wireless communications, including text messages, instant messages and e-mails sent and/or received by a public employee or school official using their Board-owned WCD may constitute public records if the content of the message concerns District business, or an education record if the content includes personally identifiable information about a student. Wireless communications that are public records are subject to retention and disclosure, upon request, according to Policy 8310. Wireless communications that are student records should be maintained pursuant to Policy 8330. Finally, wireless communications and other electronically stored information (ESI) stored on the staff member's Board-owned WCD may be subject to a Litigation Hold pursuant to Policy 8315. Staff are required to comply with District requests to produce copies of wireless communications in their possession that are either public records or education records, or that constitute ESI that is subject to a Litigation Hold.

Except in emergency situations, employees are prohibited from using WCDs to capture, record or transmit the words (i.e. audio) and/or images (i.e. pictures/video) of any student, staff member or other person in the school or while attending a school-related activity, without express prior notice and explicit consent for the capture, recording or transmission of such words or images. Using a WCD to take or transmit audio and/or pictures/video of an individual without his/her consent is considered an invasion of privacy and is not permitted, unless authorized by the building principal or Superintendent.

At no time may any WCD be used by an employee in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated.

Employee's Responsibilities

Employees are responsible for the safekeeping, care and custody of the WCDs assigned to them. Further, employees are responsible for the cost of misuse, intentional damage or reckless loss of the WCDs provided to them.

Reasonable precautions should be taken to prevent unauthorized use/access to, or loss, damage, theft and/or vandalism to said devices. Upon resignation or termination of employment, or at any time upon request, the employee may be asked to produce the WCD for return or inspection. Employees unable to present the device in good working condition within the time period requested may be expected to bear the cost of a replacement. Employees who separate from employment with outstanding debts for equipment loss or unauthorized charges will be considered to have left employment on unsatisfactory terms and may be subject to legal action for recovery of the loss.

Prior to issuance of a Board-owned WCD, each employee shall review and sign the Board WCD Policy Statement. Each employee issued a Board-owned WCD will receive a detailed monthly statement for all charges. The employee must review the monthly statement for billing accuracy, then sign and date it verifying the employee's review and attesting that there are no charges for personal calls, text messages, instant messages or e-mails. In the event that a personal call is inadvertently made or received, or a text message, instant message or e-mail of a personal nature is sent or received on the employee's Board-owned WCD, the employee shall be billed for the actual cost of the personal calls made or received, or the text messages, instant messages or e-mails sent or received. In addition, the employee shall also be charged a portion of the monthly service fee. If the employee's service plan is all-inclusive and charges are not assessed for individual calls, text messages, instant messages or e-mails, then the employee will be charged a pro-rated share of the monthly charge. Any amount owed will be deducted from the employee's paycheck in the following pay cycle.

Any employee who abuses Board-owned WCD privileges by placing or receiving personal calls, or uses his/her Board-owned WCD to send/receive personal e-mails, text messages, or instant messages, shall be subject to disciplinary action. Use of a Board-owned WCD by an employee to access a personal e-mail account or connect to the Internet for personal business is strictly prohibited.

WCDs may not be transferred to any other employee without prior notification and approval of the Superintendent. Employees provided with a WCD understand that the WCD is owned by the Board. Any alteration or switching of WCDs must be approved in advance by the Superintendent.

Cellular telephone numbers provided by the Board, via contract with a wireless service provider/vendor, are considered business numbers of the District which shall remain and belong to the Board for its use, unless otherwise changed by the service provider/vendor or as mandated by the Federal Communications Commission. Employees are not allowed to transfer/port a previous personal cellular telephone number to a Board-owned WCD.

-Employees may not download or access any prohibited application as identified by the DMS unless a waiver for certain law enforcement officers and/or purpose is specifically requested and obtained from DMS in accordance with F.S. 112.22. Upon notice of any changes to the DMS's list of prohibited applications, District employees shall have fifteen (15) calendar days to remove such applications.

The Board may audit all Board-owned WCDs, which will include but not be limited to, a review of the detailed monthly statement upon submission after the requisite review by the employee. The detailed monthly service statements for all Board-owned WCDs as well as invoices and payment documents related to these accounts are public records and may be subject to disclosure and review.

Privacy Issues

The use of WCDs that contain built-in cameras (i.e. devices that take still or motion pictures, whether in a digital or other format) is prohibited in locker rooms, classrooms, bathrooms, and/or swimming pool.

Use of Board-owned WCDs for Personal Calls

Use of a Board-owned WCD for personal business is prohibited but there may be limited situations when personal use is justified. Employees shall not take advantage of this provision and repeated use of a Board-owned WCD for personal business will result in disciplinary action.

If unforeseen circumstances develop where employees must use their Board-issued WCD for personal reasons (i.e. to let family know that the employee will be home late, etc.), the Superintendent shall determine whether the employee should reimburse the Board.

The Board will routinely audit the phone log/record provided by employees to confirm that no personal calls were made and/or to ensure that the costs associated with any personal calls made by the employee are timely reimbursed to the Board.

The Board may withhold any unreimbursed amount from the employee's wages.

Employees will be expected to sign an agreement that allows the Board to deduct the cost of unpaid calls from the employee's paycheck.

Use of a Personal WCD While at Work

During work hours, personal communications made or received, regardless of whether on a WCD, regular telephone, or network computer, can interfere with employee productivity and/or distract others. Employees are expected to use discretion in using personal WCDs while at work. Employees are asked to limit personal communication to breaks and lunch period and to inform friends and family members of the Board's policy in this regard.

Potential Disciplinary Action/Cancellation of Board-Owned WCD

Violation of this policy may constitute just cause for disciplinary action up to and including termination. Use of the WCD in any manner contrary to local, State or Federal laws will constitute misuse, and will result in the Board immediately canceling the employee's privilege to use a Board-owned WCD and return of the device.

Legal References:
F.S. 112.22
F.S. 316.305
F.S. 316.306

Effective 07.01.2011

Adoption Date: 05.11.2011

Book	Policy Manual
Section	November 15, 2023- Initial Reading
Title	**STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS & INTERNET SAFETY**
Code	7540.03
Status	Initial Reading

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

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 school district and the community. All users must, however, exercise appropriate and responsible use of school and District technology and information systems. Users include anyone authorized by administration to use the network. This policy is intended to promote the most effective, safe, productive, and instructionally sound uses of network information and communication tools.

I. District Network & Technology Resources

The District network is defined as all computer and networked resources, including software, hardware, electronic mail systems, networked devices, cloud storage/solutions, third-party solutions managed by District and/or for which the District has contracted for services, network circuits, and services that allow connection of district computers to other computers, whether they are within the district or external to the District, including connection to the Internet with any device, regardless of whether it is District/school-issued or personal, while on school property. The Board shall maintain a system of internet content filtering devices and software controls that meet the Federal standards established in the Children's Internet Protection Act (CIPA).

II. **Internet Safety**

The District shall limit student access to the Internet:

A. to only age-appropriate subject matter and materials on the Internet;

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

C. in a manner that prohibits access by students to data or information, including so-called "hacking", and other unlawful online activities by students;

~~D.~~ 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;

D.

E. in a manner that prohibits and prevent 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;

F. 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.

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 platforms reviewed and unblocked. Upon receipt of this request, ITS will review the blocked content for compliance with this policy and applicable cyber-security laws.

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

III. Digital Citizen

The Board uses information and technology in safe, legal, and responsible ways. A responsible digital citizen is one who:

A. respects one's self;

Users will select online names that are appropriate and will consider the information and images that are posted online.

B. respects others;

Users will refrain from using District network systems and social media to bully, tease, or harass other people.

C. protects one's self and others;

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

D. respects authorship;

Users will properly reference or cite to work, websites, books, media, etc., used in any student work.

E. protects intellectual property.

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

IV. Student Responsible Use

Responsible use of the District's network is expected to be ethical, respectful, academically honest, and supportive of the school's mission. Each user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators, their designees, or contracted entities may review files and communications on the District's network and related systems (including but not limited to electronic mail, managed chat applications, and network or cloud storage) to ensure that users are using the system in accordance with District policy and administrative procedures and guidelines. Users do not have any expectation of privacy in files stored electronically on the District's network and related systems which may be subject to disclosure pursuant to Florida's Public Records Act.

Student users shall comply with the following rules of network etiquette, including but not limited to:

A. Use of the District's network, electronic devices, and social media must be consistent with the District's educational objectives, mission, and curriculum; all users of the District network are bound by the guidelines and stipulations set forth within the Network Security Standards, which are posted on the District's website.

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

C. Students shall not use another individual's account. Users must not share their password with anyone, engage in activities that would reveal anyone's password, or allow others to access a computer that the user 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 maintaining their passwords private and secure.

D. Transmission of any material in violation of any local, Federal, and State laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material, and defamatory, threatening, bullying, discriminating, slanderous, offensive, harassing, cyberstalking, or obscene material.

   Obscene material is material which:

   1. the average person, applying contemporary community standards, would find, taken as a whole, appeals solely to the prurient interest; and

   2. depicts or describes, in a patently offensive way, sexual conduct as defined in State law (F.S. 847.001(11); and

   3. taken as a whole, lacks serious literary, artistic, political, or scientific value.

E. Intentional or unintentional use of District resources to access or process, proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.

F. The network may not be used to send or receive messages that discriminate on any protected basis as delineated in the Board's Anti-Discrimination Policy 5517.

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

H. Cyberbullying is prohibited at all times, on school grounds or off, whether using District-owned equipment and networks, social media or personally owned equipment and broadband connections of any kind. See Policy 5517.01, *Bullying and Harassment*.

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

J. Use of District or network resources for commercial activities, product advertisement, and religious or political campaigning, lobbying, or solicitation is prohibited.

K. Accessing unmanaged or non-sanctioned chat rooms or instant messaging using the District's network is prohibited.

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

M. Users 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.

N. Files stored on District-managed networks and hardware are the property of the District and may be monitored or inspected by administrators, their designees, or contracted entities at any time.

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

V. **Procedures for Use**

A. Student users must always get permission from teachers or facilitators before using the network or accessing any specific file or application.

B. Students shall receive education 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; and

3. the consequences of unauthorized access (e.g., hacking, cyber-bullying, 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.

C. All student users (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.

D. A student may possess a wireless communications device while the student is on school property or in attendance at a school function; however, a student may not use a wireless communications device during instructional time, except when expressly directed by a teacher solely for educational purposes. If authorization has been specifically given by the school for use within the District's educational mission, students may bring their own device such as a laptop computer, a smartphone, or cellular phone, or any other device that may access the school or District network. However, teachers shall have authority to designate an area for wireless communications devices during instructional time. The District/school is not responsible if a student's wireless communication or any electronic device is damaged, lost, or stolen. Students will be notified of any additional responsibilities for use of these devices.

E. Students shall be prohibited from utilizing the data access capabilities of a wireless communications device, 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 school personnel.

VI. **Social Media**

Social media is defined as internet-based applications (such as Facebook, Twitter, etc.) that facilitate interactive dialogue between users. The Board encourages the use of social media technologies and platforms to promote District schools and programs and to transmit information relevant to the District and/or schools.

Board members, District offices, and schools are permitted to create social media accounts that follow District guidelines, to share the school's accomplishments with students, parents, businesses and the community. Students and parents shall be provided the opportunity to opt-out of having their child's identification or photographic image posted to these sites. The opt-out form must be maintained in the student's cumulative file.

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 or the Board, or its members. Use of the District's network and/or equipment 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 and violation of this or any other Board policy may result in suspension of network access and/or discipline in accordance with Policy 5500, *Student Conduct and Discipline* and the *Code of Student Conduct*. Inappropriate material and use is defined as any material or use that is inconsistent with the goals, objectives, and policies of the educational mission of the District. User access may be affected if the school, Regional Center, or District administrator determines that a user has used the Internet or District network in an inappropriate or unacceptable manner. Students may also be subject to other legal action.

VIII. Board Liability

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

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

B. use of information obtained via the Internet, including any damages a user may incur including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors;

C. the accuracy or quality of information obtained through the Internet;

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

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

F. personally owned 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.

~~IX.~~

Effective 07.01.2011
Revised 07.18.2012
Revised 06.17.2015
Revised 03.15.2017
Revised 08.16.2023

Legal References:
F.S. 112.22
F.S. 748.048
F.S. Ch. 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
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, 54.501, 54.502, 54.503, 54.504, 54.505, 54.506, 54.507
47 C.F.R. 54.508, 54.509, 54.511, 54.513, 54.514, 54.515, 54.516, 54.517
47 C.F.R. 54.518, 54.519, 54.520, 54.522, 54.523

Adoption Date: 05.11.2011

Book	Policy Manual
Section	November 15, 2023- Initial Reading
Title	**STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS**
Code	7540.04
Status	Initial Reading

7540.04 - **STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS**

The School Board provides access to a large variety of technology and network resources which provide multiple opportunities to enhance learning and improve communication within the school district and the community. All users must, however, exercise appropriate and responsible use of school and District technology and information systems. Users are defined as anyone authorized by administration to use the network. This includes, but is not limited to: staff, vendors, contractors, and volunteers. For purposes of this policy, the term "staff" shall include all District employees and non-student users, such as charter school employees, contractors, and/or volunteers. This policy is intended to promote the most effective, safe, productive, and instructionally sound uses of network information and communication tools.

I. District Network & Technology Resources

The District network is defined as all computer and networked resources, including software, hardware, electronic mail systems, networked devices, cloud storage/solutions, third-party solutions managed by District staff and/or for which the District has contracted for services, network circuits, and services that allow connection of District computers to other computers, whether they are within the district or external to the District, including connection to the Internet with any device, regardless of whether it is District/school-issued or personal, while on school property. The Board shall maintain a system of internet content filtering devices and software controls that meet the Federal standards established in the Children's Internet Protection Act (CIPA).

II. **Digital Citizen**

The Board uses information and technology in safe, legal, and responsible ways. A responsible digital citizen is one who:

A. respects one's self;

Users will select online names that are appropriate and will consider the information and images that are posted online.

B. respects others;

Users will refrain from using District network systems and social media to bully, tease, or harass other people.

C. protects one's self and others;

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

D. respects authorship;

Users will properly reference or cite references including work, websites, books, media, etc., used in the development of any presentations, curriculum, etc.

E. protects intellectual property.

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

III. Staff Responsible Use

Responsible use of the District's network is expected to be ethical, respectful, academically honest, and supportive of the District's educational mission and objectives. Each user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators, their designees, or contracted entities may review files and communications (including but not limited to electronic mail, managed chat applications and network or cloud storage) to ensure the system is being used in accordance with District policy and administrative procedures and guidelines. Users do not have any expectation of privacy in files stored electronically on the District's network and related systems which may be subject to disclosure pursuant to Florida's Public Records Act.

All users are expected to use the network to take any action and/or communicate any language that the employee or student could not take or communicate in person. Prohibitions in applicable Federal, State, and/or local law or regulation, collective bargaining agreements, and Board policies are included. Additionally, there is no expectation of privacy in the use of e-mail or network communications when such communications occur over District provided equipment by District staff, students, or others (See Policy 7540.05).

Users are expected to comply with the rules of network etiquette, including but not limited to:

A. Use of the District's Network and electronic devices must be consistent with the District's educational objectives, mission, and curriculum; all users of the District's network are bound by the guidelines and stipulations set forth within the Network Security Standards, which are posted on the District's website.

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

C. Staff shall not use another individual's account. Users must not share their password with anyone, engage in activities that would reveal anyone's password, or allow others to access a computer that the user is logged on to. Attempting to log in to the system as any other user is prohibited. Staff is expected to act with due care in maintaining their passwords private and secure.

D. Transmission of any material in violation of local, Federal, and/or State laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material, and defamatory, threatening, bullying, discriminating, slanderous, offensive, harassing, cyberstalking, or obscene material.

   Obscene material is material which:

   1. the average person, applying contemporary community standards, would find, taken as a whole, appeals solely to the prurient interest; and

   2. depicts or describes, in a patently offensive way, sexual conduct as defined in State law (F.S. 847.001(11)); and

   3. taken as a whole lacks serious literary, artistic, political, or scientific value.

E. Intentional or unintentional use of District resources to access or process proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.

F. The network may not be used in any way that discriminates on any protected basis as delineated in the Board's anti-discrimination policies.

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

H. Downloading or using prohibited applications as identified by the Florida Department of Management Services (DMS) is prohibited.

~~H.~~I. Downloading pictures, sounds, video clips, text documents, or any material without authorization and without confirmation is prohibited unless the employee has the right to use it or has obtained permission from the copyright owner.

~~I.~~J. Downloading games, video files, audio files, or streaming media without educational value or without prior authorization by an administrator is prohibited.

~~J.~~K. Uploading, downloading, transferring, or installing software applications, images, texts, video files, and digital music files without authorization is prohibited.

~~K.~~L. Use of District resources for commercial activities, product advertisement, or religious or political campaigning, lobbying, threats, suggestions of violence, or solicitation is prohibited.

~~L.~~M. Accessing unmanaged or non-sanctioned chat rooms or instant messaging while using the District's network is prohibited.

~~M.~~N. Bypassing the District's content filter without authorization is strictly prohibited.

~~N.~~O. Users 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.

~~O.~~P. Use of the network in such a way that other users would be unable to get the full benefit of information available is prohibited. This includes, but is not limited to: running applications that deny the network's services to others, tying up computers without a legitimate educational, District or school business purpose while others are waiting, damaging software or hardware so that others are unable to use it, or any conduct that would be prohibited by State law (F.S. 815.06).

~~P.~~Q. Software, services, games, applications, video or audio files, or streaming media obtained without permission may never be installed, uploaded/downloaded or utilized on District/school devices without prior authorization by Information Technology Services (ITS).

~~Q.~~R. Cyberbullying is prohibited at all times, on campus or off, whether using District-owned equipment and networks or personally owned equipment and broadband connections.

~~R.~~S. Using the District's wireless equipment while on District property to connect without authorization to any wireless networks other than those provided by the District is prohibited. External signals will not provide content filtering and access to private networks may be illegal.

~~S.~~T. Files stored on or accessed via District-managed networks and hardware as defined previously in this policy are the property of the District and may be monitored or inspected by administrators, their designees, or contracted entities at any time. Materials published electronically must be for educational purposes. Administrators should monitor these materials to ensure compliance with content standards.

IV. Procedures for Use

A. School, Region, and District administrators are authorized to determine appropriate and acceptable use pursuant to this policy.

B. Staff members shall participate in professional learning and provide instruction to students that includes:

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

2. the dangers inherent in disclosing personally identifiable information online and/or passwords; and

3. the consequences of unauthorized access (e.g., hacking, cyberbullying), unlawful or inappropriate online activities, and other cyber threats.

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

C. Staff is required to affirm that they have read and agree to comply with this policy on a yearly basis.

D. Personal use of the District's network, including e-mail and the Internet, is permitted as long as it does not interfere with an employee's duties, a student's learning activities and/or system operation and complies with all District policies and standards, State and/or Federal law, and Florida's Code of Ethics for the Education Profession.

E. Blogging is the activity of writing entries in, adding material to, or maintaining a "weblog". A podcast is an audio show or series available for download or streaming via the internet (similar to a radio show). Employees shall not engage in blogging activities, recording podcasts or engaging in other similar communication forums during working hours or use District-owned equipment for blogging, podcast, or similar/related activities unless it is included as a legitimate part of classroom instruction or related to a school sanctioned educational program or activity. During non-working hours, staff members are representatives of the District and should behave in a manner that does not disrespect or discredit the education profession. Unless engaging in an officially sanctioned District activity, employees using "blogs", podcasts, and/or similar communication forums should clearly specify that any opinions or statements are the employee's own and do not reflect the views of the District. Staff is prohibited from using School District logos, school mascots, and other official symbols.

F. Staff is not permitted to use or disclose personally identifiable student information and information contained in student education records without parental consent (See Policy 8330). Staff members may not disclose or post confidential employee information.

V. **Social Media**

Social media is defined as internet-based applications (such as Facebook, Twitter, etc.) that facilitate interactive dialogue between users. The Board encourages the use of social media technologies and platforms to promote District schools and programs and to transmit information relevant to the District and/or school(s).

Board members, the District offices, and schools are permitted to create social media accounts, in compliance with District guidelines, to share District and school accomplishments with students, parents, businesses, and the community. Students and parents shall be provided the opportunity to opt-out of having their child's identification or photographic image posted to these sites. The opt-out form must be maintained in the student's cumulative file.

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

Some social media sites allow users to become a "friend" or otherwise associate their "profiles" in a more private and personal arrangement which may mask inappropriate conduct. Staff members are discouraged from "friending" students on Facebook or other similar websites/applications, other than for the limited purpose of communications necessary to further educational objectives.

Employees shall not use District or school social media for collective bargaining purposes or union organizational activities, but may use non-District social media for these purposes.

The District shall prohibit 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, extracurricular organization, or athletic team.

VI. Violations and Sanctions

Inappropriate use and violation of this or any other Board policy may result in suspension of network access and/or employee discipline. Inappropriate material and use is defined as any material or use that is inconsistent with the goals, objectives, and policies of the educational mission of the District. Any user can be denied access temporarily or permanently if the school, Region, or District administrator determines that a user has used the Internet or District network in an inappropriate or unacceptable manner. Staff may be disciplined or subject to legal action for violations of this policy.

VII. Board Liability

The Board is not responsible for, and cannot be held liable for:

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

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

C. use of any information obtained via the Internet, including any damages a user may incur including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors, or omissions;

D. the accuracy or quality of information obtained through the network;

E. issues or damage caused by the connection of personal devices to the District's network or improper use of the Districts network or equipment; or

F. personally owned devices that are damaged, lost, or stolen.

VIII. 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.

IX. **Training**

Annual training on cybersecurity will be conducted for District employees.

Effective 07.01.2011
Revised 07.18.2012
Revised 06.17.2015
Revised 03.15.2017
Revised 12.09.2020
Revised 08.16.2023
Technical Correction 09.11.2023

Legal References:
F.S. 112.22
F.S. 748.048
F.S. 847, et. seq.
F.S. 1001.41
F.S. 1012.32
P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h),(1), Communications Act of 1934, as amended (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
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, 54.501, 54.502, 54.503, 54.504, 54.505, 54.506, 54.507
47 C.F.R. 54.508, 54.509, 54.511, 54.513, 54.514, 54.515, 54.516, 54.517
47 C.F.R. 54.518, 54.519, 54.520, 54.522, 54.523

Adoption Date: 05.11.2011