Office of Superintendent of Schools
Board Meeting of October 14, 2026

September 30, 2026

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

SUBJECT: **FINAL READING: PROPOSED AMENDMENTS TO SCHOOL BOARD POLICIES 7540.02, *DIGITAL APPLICATIONS AND SERVICES*, AND 7540.04, *STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS***

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

LINK TO STRATEGIC PLAN: **INFORMED, ENGAGED, & EMPOWERED STAKEHOLDERS**

Consistent with the Board's responsibility to review and amend its policies, and pursuant to Board action, authorization is requested for the Superintendent to amend School Board Policies 7540.02, *Digital Applications and Services*, and 7540.04, *Staff Responsible use of Technology, Social Media, and District Network Systems***.**

Policies 7540.02 and 7540.04 are proposed for amendment in response to June 2026 Item H-4, "21st Century Social Media Account Policy," proffered by School Board Member Luisa Santos, which directed the Superintendent to, among other things, "initiate rulemaking, as necessary, to establish standards regarding account naming conventions, credential management, account ownership, continuity planning, and administrative oversight for District-affiliated social media accounts, including: District leadership (Superintendent and Cabinet), central bureaus and departments, and primary school-site accounts." Additionally, in accordance with August 2026 Item H-10, "Feasibility of Expanding Principal Autonomy and Support for School-Level Marketing," proffered by School Board Member Daniel Espino, the proposed policy amendments account for school-level marketing, recruitment, websites, social media, community outreach, student privacy, branding, use of District resources, and school principals' autonomy and flexibility.

Pursuant to these items, Policy 7540.02 is proposed for amendment to clarify that District social media accounts, including those created by individual schools and individual employees acting in their official capacities, are subject to oversight by the District's Office of Communications to ensure that District branding, identification elements, and operational standards are followed. The policy would be amended to require the Superintendent to develop a digital toolkit to be made available to all departments, schools, and employees creating or developing social media accounts; to provide that District social media account creation, closure or transfer requires approval from the Office of Communications; to require that account credentials are retained both by the account-holder and the Office of Communications to maintain continuity of operations; to require that District social media account names and handles bear a reasonable connection to the employee, office, or school to which the account is dedicated; to prohibit confidential and exempt information (such as protected student information) from being posted on these accounts; to clarify the types of content the District reserves the right to remove from these accounts, consistent with applicable law; and to require that before any action is taken affecting the public's access to District social media accounts (e.g., removing posts or comments), prior approval must be secured from the Office of Communications. The policy would further specify that is not intended to limit a principal's autonomy and flexibility to engage in school-level marketing, recruitment, website development, social media engagement, community

outreach, branding, and the use of District resources for these purposes.

Policy 7540.04 is similarly proposed for amendment to ensure that employees who conduct official District business on social media do so in a manner that complies with applicable law and Policy 7540.02. The proposed amended policy would clarify that the District retains proprietary and editorial control over approved District social media accounts created by employees in the course and scope of their employment, including the right to alter or remove content generated on these accounts and to restrict or remove an employee's account-management privileges. The policy would also prohibit mixed-use social media accounts, requiring that personal social media accounts be used only for personal matters, and that District social media accounts be used only for District business. Finally, the policy would clarify that no confidential or exempt information (e.g., protected student information) may be posted on an employee's personal social media account.

The Notice of Intended Action was published in the Miami Herald on September 14, 2026, and posted in various places for public information and mailed to various organizations representing persons affected by the adopted and amended Board policies and individuals requesting notification. The time to request a hearing or protest the adoption and amendment of these policies has elapsed.

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.

RECOMMENDED: That The School Board of Miami-Dade County, Florida, amend School Board Policies 7540.02, *Digital Applications and Services*, and 7540.04, *Staff Responsible use of Technology, Social Media, and District Network Systems*, and authorize the Superintendent to file the policies with The School Board of Miami-Dade County, Florida, to be effective October 14, 2026.

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on September 9, 2026, its intention to amend School Board Policies 7540.02, *Digital Applications and Services*, and 7540.04, *Staff Responsible use of Technology, Social Media, and District Network Systems*, at its meeting of October 14, 2026.

PURPOSE AND EFFECT: School Board Policies 7540.02, *Digital Applications and Services*, and 7540.04, *Staff Responsible use of Technology, Social Media, and District Network Systems*, are proposed for amendment in response to Board action directing updates to social media policies while preserving principals' autonomy and flexibility in marketing.

SUMMARY: Policy 7540.02 is proposed for amendment to clarify that all District social media accounts are subject to oversight by the District's Office of Communications (OOC). The policy would be amended to require the Superintendent to develop a digital toolkit to be made available to all District social media account holders; to provide that account creation, transfer, and closure require OOC approval; to require that account credentials be retained both by the account-holder and the OOC; to require that District social media account identifiers bear reasonable connections to the account-holder or program; to prohibit confidential and exempt information from being posted on these accounts; to clarify the types of content the District reserves the right to remove from these accounts; and to require OOC approval before any action is taken affecting the public's access to these accounts. The policy would also clarify that it is not intended to abridge principal flexibility and autonomy or First Amendment rights. Policy 7540.04 would be revised to clarify that employees conducting District business on social media must do so in a manner that complies with applicable law and Policy 7540.02; to clarify that the District retains proprietary and editorial control over approved District social media accounts created by employees in the course and scope of their employment; to prohibit mixed-use social media accounts, requiring that District social media accounts be used only for District business; and to clarify that confidential or exempt information cannot be posted on personal social media accounts.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: Fla. Stat. ss. 1001.32(2); 1001.41(1)–(2); 1001.42(6), (8); 1001.51(4), (7).

LAW IMPLEMENTED, INTERPRETED, OR MADE SPECIFIC: Fla. Stat. Ch. 119; Fla. Stat. ss. 1003.02; 1012.27(7).

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF October 14, 2026, 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 October 6, 2026, 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	October 14, 2026 – Final Reading
Title	DIGITAL APPLICATIONS AND SERVICES
Code	7540.02
Status	Final Reading

7540.02 – **DIGITAL APPLICATIONS AND SERVICES**

Users are authorized to create content on digital applications (apps)/services, as defined in Policy 7540, to promote school activities and inform stakeholders and the general public about District news and operations. Content created on digital apps/services must comply with this policy and constitute public records that will be archived.

I. **Creation of Content on Digital Apps/Services**

A. Digital apps/services are used to communicate and transfer information and data that allow students to perform actions and tasks that assist them in attaining educational achievement goals and objectives; enable staff members to monitor and assess their students' progress; and allow staff members to perform other tasks related to their employment. Digital apps/services are also used to facilitate communication to, from, among and between staff members, students, parents, and third parties. Content on digital apps/services should be created with the understanding that both internal and external audiences will be viewing the content.

B. Content on digital apps/services created by staff members and students of the District may be published on the Internet and/or presented for public consumption. The creation of content on digital apps/services by students must be done under the supervision of an instructional staff member and must reflect the professional image of the District, its employees, and students. All content must be consistent with the School Board's mission statement and is subject to prior approval of the Superintendent prior to any publication.

C. The Board authorizes the use of digital apps/services to supplement and enhance learning opportunities for students either in the classroom or for extended learning outside the classroom.

D. The Superintendent shall prepare procedures defining the standards of permissible use.

II. Requirements of Content Posted on Digital Apps/Services

A. The purpose of digital apps/services is to educate, inform, and communicate. The information contained within digital apps/services should reflect and support the Board's mission statement, educational philosophy, and the school improvement process.

B. In developing content for digital apps/services, the following criteria should be used:

1. Educate

   Content should be suitable for and usable by students and teachers to support the curriculum and the Board's objectives as listed in the Board's strategic plan.

2. Inform

   Content may inform the community about the school, teachers, students, or departments, including information about curriculum, events, class projects, student activities, and departmental policies.

3. Communicate

   Content may communicate information about the plans, policies, and operations of the District to members of the public and other persons who may be affected by District matters.

C. All links included on digital apps/services must meet the above criteria and comply with State and Federal laws (e.g., copyright laws, Children's Internet Protection Act, and Children's Online Privacy Protection Act). Only content that is verified to be in the public domain or properly licensed may be used on digital apps/services.

D. Under no circumstances are digital apps/services to be used for lobbying for candidates for public office, or to provide financial gains for any individual, except as the Superintendent authorizes. Content linked from or hosted on digital apps/services also may not:

1. include statements or other items that support or oppose a candidate for public office, the investigation, prosecution or recall of a public official, or passage of a tax levy or bond issue;

2. link to a website of another organization if the other website includes such a message; or

3. communicate information that supports or opposes any labor organization or any action by, on behalf of, or against any labor organizations.

E. Before any statement that supports a tax referendum proposed by the District is posted on the District website, or on any web pages linked to the District website, the Board shall adopt a resolution at a public meeting ~~declaring that such statement serves a public purpose~~supporting the proposed referendum.

F. School websites must be hosted on District-approved platforms.

III. Social Media

A. 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. District social media accounts include those created by individual departments and schools, and individual employees acting in their official capacities.

B. Board members, District offices, and schools are permitted to create social media accounts that follow District guidelines to share the District's and schools' messages with students, parents, businesses and the community. Use of social media accounts for these purposes must comply with Policy 8330, *Student Information, Records, and Privacy Rights*.

C. The Superintendent shall develop a digital toolkit to be made available to all departments, schools, and employees creating or developing social media accounts.

D. District social media accounts shall be approved and overseen by the District's Office of Communications or, if the account is for a school site, by the corresponding Region. All account credentials shall be provided to ensure continuity of operations.

E. District social media accounts are intended to provide accessible, relevant information on specific topics to target audiences. These accounts are not intended to provide a forum for unrelated

commentary or expression. Accordingly, the District reserves the right to remove any comment or post that contains:

1. Obscene, vulgar, or sexually explicit content;

2. Threats of any kind, or advocacy for criminal acts or other illegal behavior;

3. Content that constitutes unlawful discrimination or harassment;

4. Content that may be reasonably considered defamatory;

5. Content that is clearly off topic for the social media account or post; and

6. Campaign materials of any kind, political or otherwise, or links to third-party sites or advertisements.

All District social media accounts must conspicuously display a notice advising users of these restrictions and warning users that repeated violations may result in their access to the account being limited or restricted. Automated moderation tools are allowed to be used to the extent they are applied uniformly and are reasonable and viewpoint neutral.

F. District social media account names and handles must bear a reasonable connection to the employee, office, or school to which the account is dedicated.

G. No confidential or exempt information may be posted on a District social media account, except as authorized by the Office of Communications.

H. Before taking any action affecting the public's access to District social media accounts (e.g., removing posts or comments or limiting access), prior approval must be secured from the Office of Communications. Any such action must be reasonable and viewpoint neutral in light of the District social media account's purpose.

I. District and school-affiliated social media accounts must appropriately indicate their official affiliation with Miami-Dade County Public Schools. Accounts that fail to maintain required District branding, identification elements, or operational standards may be deemed unauthorized or personal accounts, subject to review or administrative action.

J. For all operational requirements, branding standards, and account management procedures, staff must consult and adhere to the District Social Media Guidelines.

IV. Reservation of Proprietary Rights

A. The Board retains all proprietary rights related to the design of websites and/or pages that are hosted on the District network, along with other content on digital apps/services, absent written agreement to the contrary. This includes ownership of all District social media accounts.

B. Any District social media account creation, closure, or transfer requires prior approval from the Office of Communications. Anyone managing a District social media account must transfer management and account credentials to the Office of Communications or to the corresponding Region upon separating from the District so the account can be transferred or closed, as applicable.

C. Content on District social media accounts may constitute public records. Accordingly, District employees are expected to retain such records and transmit them to the District upon request and upon separating from the District. The applicable records retention period is listed in Schedule GS1-SL of the Florida Department of State General Records Schedule.

V. Confidentiality of Student Content on Digital Apps/Services

A. When content on digital apps/services includes a photograph or information relating to a student, the Board will follow Policy 8330.

B. Prior written parental permission is necessary for a student to be identified by name on digital apps/services and social media.

C. Students who want their class work to be displayed on a school's website (or on other digital apps/services) must have written parent permission and expressly license its display without cost to the Board.

VI. Digital App/Service Accessibility

A. In accordance with Federal and State disability laws and regulations, the District is committed to providing persons with disabilities an opportunity equal to that of persons without disabilities to access digital apps/services unless doing so results in a fundamental alteration or an undue financial and administrative burden.

B. The District will adhere to the technical standards of compliance identified in the Accessibility Statement on the District homepage. The District measures the accessibility of online content and functionality according to the version of the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG) required by federal regulations.

C. The District's Americans with Disabilities Act (ADA) Office will review content available on digital apps/services that are related to the District's programs, benefits and/or services for compliance with this section.

D. Any user of the District's digital apps/services who wishes to report an accessibility issue may contact the District's ADA Office with concerns and/or file a formal complaint using the procedures set out in Policy 1362.02, Policy 3362.02, or Policy 4362.02.

VII. Training

The District will provide periodic training for its staff members who are responsible for creating or distributing information with online content so that these staff members are aware of this policy and understand their roles and responsibilities with respect to web design, documents, and multimedia content.

VIII. Scope and Severability

This policy is not intended to limit a principal's autonomy or flexibility to engage in school-level marketing, recruitment, website development, social media engagement, community outreach, and branding, and to use District resources for these purposes. Additionally, this policy shall not be construed or applied in a manner that abridges the First Amendment rights of students, employees, or the public. If any section, paragraph, sentence, clause, phrase, or word of this policy is for any reason held by a court to be unconstitutional, inoperative, or void, it is intended that, to the maximum extent practicable, such holding shall not affect the remainder of this policy.

Effective 07.01.2011
Revised 03.15.2017
Revised 07.24.2024

© Miami-Dade County Public Schools 2024

Legal References:
F.S. 104.31(1)(a)
F.S. 110.233(2)
F.S. 110.233(4)
F.S. 112.313(6)

F.S. 1001.32(2)
F.S. 1001.42
28 C.F.R. Part 35
P.L. 106-554, Children's Internet Protection Act of 2000

Adoption Date: 05.11.2011

Book	Policy Manual
Section	October 14, 2026 – Final Reading
Title	STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS
Code	7540.04
Status	Final 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 District and the community. All staff members 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 & Technology 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. **Digital Citizen**

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

A. Respects oneself:

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

B. Respects others:

Staff members will refrain from using the District network and social media to bully, tease, or harass other people.

C. Protects oneself and others:

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

D. Respects authorship:

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

E. Protects intellectual property:

Staff members 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 music files) without specific permission.

III. Staff Responsible Use

A. 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 staff member has the responsibility to respect every other person in our community and on the Internet.

B. District technology will be treated as an extension of the physical school and workspace. Administrators, their designees, or contracted entities may review files and communications on the District technology and related systems (including but not limited to electronic mail, managed chat applications and network or cloud storage) to ensure that staff members are using these systems in accordance with Board policy and administrative procedures and guidelines. Staff members have no expectation of privacy in files stored electronically on District technology and related systems, including the e-mail system, which may be subject to disclosure pursuant to Florida's Public Records laws (see also Policy 7540.05).

C. No staff member can use the District's network to take any action and/or communicate any language that the staff member could not take or communicate in person, or that the staff member is prohibited from taking or communicating under applicable Federal, State, and/or local

laws or regulations, collective bargaining agreements, and Board policies.

D. Staff members are expected to comply with the following rules of network etiquette, including but not limited to:

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

2. Any staff member 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. Staff members shall not use other individuals' accounts or log in to the system as any other user; share their passwords with anyone; engage in activities that would reveal anyone's password; or allow others to access a computer that the staff member is logged on to. Attempting to log in to the system as any other user is prohibited. Staff members are expected to act with due care in keeping their passwords private and secure.

4. Transmission of any material in violation of 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 (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's network may not be used in any way that discriminates on any protected basis as delineated in the Board policies prohibiting discrimination (see Policy 1362, Policy 3362, Policy 4362, and Policy 5517).

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

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

9. Downloading copyrighted pictures, sounds, video clips, text documents, or any material without authorization and without confirmation is prohibited unless the staff member has the right to use it or has obtained permission from the copyright owner.

10. Downloading, uploading, transferring, streaming or installing or utilizing software applications, services, images, texts, games, video files, audio files, or media on District technology without a legitimate District purpose and without prior authorization by an administrator and Information Technology Services (ITS) is prohibited.

11. The creation of digital applications/services using District technology must be done in compliance with Board policies and District procedures (see Policy 7540.02). ITS reserves the right to disable or remove such digital applications/services at its discretion.

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

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

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

15. Staff members 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. Use of the District's 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 District's network's services to others; using computers for an unreasonable amount of time without a legitimate District 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 (see F.S. 815.06).

17. Cyberbullying is prohibited at all times, on or off District property, whether using District technology, personal devices, or other broadband connections.

18. Creating a deepfake is prohibited unless authorized by an administrator for a legitimate District purpose.

19. Using District technology 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.

20. Files stored on or accessed via District technology may be monitored or inspected by administrators, their designees, or contracted entities at any time. Materials published electronically must be for legitimate District purposes. Administrators should monitor these materials to ensure compliance with content standards.

IV. **Additional Requirements**

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 and/or information to students that includes:

1. the 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;

3. the consequences of prohibited acts (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; and

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

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

D. Personal use of District technology, including e-mail and the District's network, 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 Board policies and standards, State and/or Federal

laws, and Florida's Code of Ethics for the Education Profession.

E. Staff members shall not engage in blogging activities, recording podcasts or engaging in other similar communication forums during working hours or use District technology for blogging, recording podcasts, or similar/related activities unless it is included as a legitimate part of classroom instruction or for legitimate District purposes. 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 (see section II., above). Unless engaging in an officially sanctioned District activity, staff members using blogs, podcasts, and/or similar communication forums should clearly specify that any opinions or statements are the staff member's own and do not reflect the views of the District. Staff members are also prohibited from using District logos, school mascots, and other official symbols for non-District purposes.

F. Cameras on staff members' personal devices may not be used in any unethical or illegal manner; to photograph or record another person who has a reasonable expectation of privacy without that person's knowledge and consent; in a way that would violate copyright laws; to harass, intimidate, or bully another person or to invade another person's privacy; or in any locker room, restroom, or any other place where other people have a reasonable expectation of privacy, unless expressly authorized by an administrator for a legitimate District purpose.

G. Staff members are prohibited from using or disclosing 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**

A. Staff members shall comply with Policy 7540.02, *Digital Applications and Services*, in creating any social media account for official District business. These social media accounts are intended to convey District-related matters in a factual, objective manner, without editorialization. The District retains all proprietary rights and editorial control over these accounts.

B. Staff members who post on approved District social media accounts are doing in their official capacities and within the course and scope of their employment. The District retains the right to alter or remove any content generated on these accounts and to restrict or remove any staff member's account-management privileges.

C. Staff members are prohibited from creating mixed-use social media accounts. Personal social media accounts shall not be used for official

District business, and District social media accounts shall not be used for personal matters. Staff members are encouraged to place disclaimers on their personal social media accounts indicating that the account is personal and that the views expressed are the staff member's own.

D. No confidential or exempt information may be posted on a staff member's personal social media account.

E. When using social media, staff members shall comply with the same responsible use rules outlined above for Internet and District network use, including but not limited to, compliance with Policy 8330. In addition, staff members 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. The use of District time and/or equipment for personal social media activities is prohibited. Staff members may be disciplined by the District for ~~inappropriate~~ social media behavior that violates Board policy, even if it occurs off District property. Inappropriate personal communications using social media is prohibited

F. Staff members are discouraged from "friending" or messaging students on social media or through other similar websites/applications, other than for legitimate District purposes.

G. Staff members 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.

H. The District shall prohibit the use of the TikTok platform or any successor platform on District technology, 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.

VI. Violations and Sanctions

Inappropriate use of District technology or the District's network and violations of this or any other Board policy may result in suspension of District network access and/or employee discipline. Any staff member can be denied access temporarily or permanently if the school, Region, or District administrator determines that the staff member has used the Internet or District network in an inappropriate or unacceptable manner. Staff members 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 use of the District's network or social media activity;

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

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

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

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

F. personal 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

Upon commencing employment with the District, new or returning staff members will be required to complete cybersecurity training within thirty (30) days. Additionally, all staff members shall participate in training on cybersecurity at least annually.

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
Revised 12.20.2023
Revised 07.24.2024

© Miami-Dade County Public Schools 2024

Legal References:
F.S. 112.22
F.S. 748.048
F.S. 847, et seq.

F.S. 1001.41
F.S. 1012.32
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 (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 - 54.509, 54.511, 54.513 - 54.520, 54.522, 54.523

Adoption Date: 05.11.2011