

Office of Superintendent of Schools
Board Meeting of July 18, 2012

July 2, 2012

Financial Services
Richard H. Hinds, Chief Financial Officer

**SUBJECT: PROPOSED AMENDMENT OF BOARD POLICIES: FINAL
READING POLICY 7540.03, STUDENT NETWORK AND
INTERNET ACCEPTABLE USE AND SAFETY; AND POLICY
7540.04, STAFF NETWORK AND INTERNET ACCEPTABLE
USE AND SAFETY**

**COMMITTEE: INNOVATION, EFFICIENCY, AND GOVERNMENTAL
RELATIONS**

LINK TO STRATEGIC FRAMEWORK: FINANCIAL EFFICIENCY/STABILITY

The School Board of Miami-Dade County, Florida, announced on June 13, 2012, its intention to amend Board Policy 7540.03, Student Network and Internet Acceptable Use and Safety. The proposed policy changes will clarify and update District standards to include social media use by students and to add standards for the coming Bring Your Own Device (BYOD) wireless District initiative.

In addition, the Board announced its intention to amend Board Policy 7540.04, Staff Network and Internet Acceptable Use and Safety. The proposed policy changes will clarify and update District standards to include social media use by staff and to add standards for the coming BYOD wireless District initiative.

The Notice of Intended Action was published in the *Miami Daily Business Review* on June 18, 2012, posted in various places for public information and mailed to various organizations representing persons affected by the amended policies and to individuals requesting notification.

The time to request a hearing or protest the amendment of these policies has elapsed.

E-201

In accordance with the provisions of the Administrative Procedure Act, these policies are presented to The School Board of Miami-Dade County, Florida, for adoption and authorization to file the policies in the official records of The School Board of Miami-Dade County, Florida.

Attached are the Notice of Intended Action and the proposed amended Board Policies. Changes from the current policies are indicated by underscoring words to be added and ~~striking through~~ words to be deleted.

RECOMMENDED: That The School Board of Miami-Dade County, Florida adopt amended Board Policy 7540.03, Student Network and Internet Acceptable Use and Safety and Board Policy 7540.04, Staff Network and Internet Acceptable Use and Safety, and authorize the Superintendent to file the policies with The School Board of Miami-Dade County, Florida, to be effective July 18, 2012.

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on June 13, 2012, its intention to amend Board Policy, 7540.03, Student Network and Internet Acceptable Use and Safety, at its meeting on July 18, 2012.

PURPOSE AND EFFECT: The purpose of the proposed Board Policy is to provide the district with a policy containing the standards and guidelines for the responsible use of district network computer systems and the Internet by staff and consequences for failure to abide by these standards.

SUMMARY: The proposed policy changes add language addressing the use of Social Media by staff and the use of personal electronic devices in the coming Bring Your Own Device (BYOD) Wireless Incentive.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING AUTHORITY IS AUTHORIZED: 1001.41 (1) (2); 1001.42 (25); 1001.43 (10) F.S.

LAW IMPLEMENTED, INTERPRETED, OR MADE SPECIFIC: 1001.41; 1001.43; 1001.51; H.R. 4577, 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; 18 U.S.C. 2256; 18 U.S.C. 1460; 18 U.S.C. 2246; 76 F.R. 56295, 56303

IF REQUESTED, A HEARING WILL BE HELD DURING THE BOARD MEETING OF July 18, 2012 which begins at 1:00 p.m. in the School Board Auditorium, 1450 N.E. Second Ave., Miami, Florida, 33132. Persons requesting such a hearing or who wish to provide information regarding the statement of estimated regulatory costs, or to provide information regarding the statement of estimated regulatory costs, or to provide a proposal for a lower regulatory alternative as provided by Section 120.541(1), Florida Statutes, must do so in writing by July 10, 2012, to the Superintendent of Schools, Room 912, at the same address.

ANY PERSON WHO WISHES 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).

A COPY OF THE PROPOSED AMENDED POLICY is 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.

Originator: Dr. Richard Hinds
Date: May 30, 2012

1 STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

2 This policy establishes responsible and acceptable use of the network as a tool for
3 learning in the District. The District ~~n~~Network is defined as all computer resources,
4 including software, hardware, lines and services that allow connection of District
5 computers to other computers, whether they are within the District or external to the
6 District. This includes connection to the Internet while on school property. In this
7 policy, Users are defined as students. No user may use the ~~n~~Network to take any
8 action ~~or receive~~ and/or communicate any language that the employee or student
9 could not take or communicate in person. ~~Users are defined as anyone authorized~~
10 ~~by administration to use the Network. This includes, but is not limited to, staff,~~
11 ~~students, parents, vendors, contractors, and volunteers.~~ Prohibitions in applicable
12 Federal, State, and/or local law or regulation, collective bargaining agreements and
13 Board policies are included. Additionally, this policy reflects that there is no
14 expectation of privacy in the use of e-mail or network communications when such
15 communications occur over District provided equipment. ~~by District employees,~~
16 ~~students, or others.~~ (See Board policies concerning privacy and e-mail).

17 **Access to the Network**

18 The District Networks gives schools the ability to share educational and research
19 resources from around the world with all students. These resources include access
20 to instructional applications, interactive collaboration between teachers, students
21 and other users, document sharing, communications of all forms with people from
22 around the world and libraries, museums and research facilities.

1 **Acceptable Use**

2 Use of the ~~an~~Network must support and be consistent with the educational objectives
3 of the District. All ~~an~~Users must comply with this policy and the standards of
4 conduct established in the District Codes of Student Conduct (Elementary,
5 Secondary, and Adult), Code of Conduct for Adult Students, Florida's Code of Ethics
6 of the Education Profession, the District Network Security Standards and School
7 Board policies regarding employee behavior.

- 8 A. Transmission of any material in violation of local, State, and Federal
9 law or regulation or Board policies is prohibited. This includes, but
10 is not limited to copyrighted or trade secret material which the
11 transmitter does not have the right to transmit, and material that is
12 threatening, bullying, discriminatory, slanderous or obscene
13 material. ~~or material protected by trade secret.~~

14
15 Obscene material is material which:

- 16 1. the average person, applying contemporary community
17 standards, would find, taken as a whole, appeals solely to the
18 prurient interest; and
- 19 2. depicts or describes, in a patently offensive way, sexual
20 conduct as defined in State law (F.S. 847.001 (11)); and
- 21 3. taken as a whole, lacks serious literary, artistic, political, or
22 scientific value.

- 23 B. Procedures for protesting instructional materials and educational
24 media as they are accessed through the Internet are governed by
25 Policy 2510.

- 26 C. Use of the Internet for political activities is prohibited.

- 27 D. Use of the ~~an~~Network for product advertisement, commercial
28 activities, political campaigning or solicitation is prohibited.

1 E. The District shall use an Internet Content Filter to
2 prevent uUser access to prohibited material.
3

4 Users of the District nNetwork are charged with notice that besides
5 obscene material, there are other potentially objectionable materials
6 available on the Internet, including sites with adult content, nudity,
7 and gambling, as well as sites advocating violence and illegal
8 activities. No content filter will ever be 100% accurate, and on
9 occasion either objectionable material may get through or non-
10 objectionable material may be blocked. It is a User's obligation to
11 immediately report these lapses.
12

13 Bypassing the District content filter without authorization is strictly
14 prohibited. The District has procedures in place to evaluate
15 requests from uUsers to block or unblock sites as necessary.
16

17 Students, parents and staff should be aware that connection to any
18 Internet or network provider not under District control may be
19 unfiltered, especially open wireless connections. The District is not
20 responsible for unfiltered content that may be viewed or downloaded
21 on District equipment that has been provided to individuals for use
22 outside District property. The District is also not responsible for
23 issues caused by the connection of personal devices to the District's
24 nNetwork or improper use of the District's nNetwork or equipment.

25 **Privilege**

26 Accessing the Internet ~~through~~ using District equipment and/or through the
27 District's Network is a privilege, not a right, and inappropriate use, including
28 violation of this rule may result in cancellation of the privilege.

29 A. School, regional center, and District administrators are authorized to
30 determine appropriate and acceptable use pursuant to this policy.

31 B. Any user account may be closed, suspended or revoked at any time
32 a school, regional center, or District administrator determines an
33 account user or holder has used the nNetwork in an inappropriate or
34 unacceptable manner in violation of this or any other applicable
35 Board policy.

1 C. Inappropriate or unacceptable use is defined as use that violates this
2 policy or the District's purpose in providing students and employees
3 safe access to the Internet and use that violates the District Codes of
4 Student Conduct (Elementary, Secondary, and Adult), Code of
5 Conduct for Adult Students, Florida's Code of Ethics of the
6 Education Profession, the District Network Security Standards, and
7 Board policies governing employee behavior, or any local, State, or
8 Federal law or regulation.

9 D. Access to the Internet from the District ~~n~~Network as a tool for
10 learning will be automatic. Parents must notify the school in writing
11 if they do not want their child to access the Internet.

12 **Monitoring**

13 ~~Administration~~ District Staff has the right to review any material on user accounts to
14 maintain adequate filespace and monitor appropriateness of material ~~accessed~~
15 transmitted through the ~~n~~Network. The District shall respect the privacy rights of
16 user accounts unless there is a violation or suspected violation of this policy.

17 **Network Etiquette**

18 All Users are expected to follow the generally accepted rules of network etiquette.
19 These standards of conduct include, but are not limited to the following:

20 A. Users should be polite. The use of abusive language is prohibited.

21 B. Use appropriate language. The use of profanity, vulgarities or any
22 other inappropriate language is prohibited.

23 C. Engaging in activities which are prohibited under local, State or
24 Federal law is prohibited.

25 D. Activities which violate the Codes of Student Conduct (Policy 5500),
26 the Code of Ethics of the Education Profession in the State of
27 Florida, the District Network Security Standards and Board policies
28 governing employee behavior, are prohibited.

29 E. Do not reveal your personal address and/or telephone number or
30 that of other ~~n~~Users unless compelled to by law.

31 F. Electronic mail (e-mail) is not guaranteed to be private. People who
32 operate the system do have access to all mail. Messages relating to
33 or in support of illegal activities will be reported to the authorities
34 without notice.

1 G. Do not use the Network in such a way that other Users would be
2 unable to get the full benefit of information available. This includes,
3 but is not limited to: running applications that deny the Network's
4 services to others, tying up computers without a legitimate
5 educational or school district or school business purpose while
6 others are waiting, damaging software or hardware so that others are
7 unable to use it, or any conduct that would be prohibited by State
8 law (F.S. 815.06).

9 H. Do not use the Network to send or receive messages that
10 discriminate based on sex, race, color, religion, ethnic or national
11 origin, political beliefs, marital status, age, sexual orientation,
12 gender, gender identity, social and family background, linguistic
13 preference, disability or that are inflammatory.

14 **Services**

15 Use of any information obtained via the Internet is at the User's own risk. The
16 District will not be responsible for any damages a User may incur. This includes,
17 but is not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries,
18 or service interruptions caused by negligence, errors, or omissions.

19 The District is not responsible for the accuracy or quality of information obtained
20 through the Network. All Users need to consider the source of any information
21 they obtain through the Network, and evaluate the accuracy of the information.

22 **Security**

23 Security on any computer network is a high priority, especially when the system
24 involves many Users.

25 A. If a User can identify a security problem on the Network, the
26 User must notify a system administrator. The User must not
27 disclose or demonstrate the problem to others.

28 B. Users must not use another individual's account without written
29 permission from that individual. Attempts to log into the system as
30 any other user will result in disciplinary action as described in
31 Disciplinary Action.

32 C. Any User that has been determined by administrators to have
33 violated this rule may be denied future access to the Internet
34 through the District Network.

- 1 D. A uUser with a history of using other computer systems in an
2 inappropriate or unacceptable manner may be denied access to the
3 District Network.
- 4 E. Users of the nNetwork will be held responsible for all activity
5 associated with the uUser's account. Users should not share their
6 passwords with anyone, engage in activities that would reveal
7 anyone's password or allow anyone to use a computer to which they
8 are logged on.
- 9 F. Accessing chat rooms or instant messaging while using the District
10 nNetwork is prohibited.
- 11 G. The use of Internet tools such as blogs and discussion boards are
12 intended for educational purposes only.
- 13 H. Downloading pictures, sounds, video clips, text documents or any
14 material without authorization and without confirmation is
15 prohibited unless that the material is not copyrighted is prohibited
16 User has the right to use it or has obtained permission from the
17 copyright owner.
- 18 I. Downloading games, video files, audio files or running streaming
19 media without educational value and without authorization by a
20 teacher or a local administrator is prohibited.
- 21 J. Uploading, Downloading or installing software applications without
22 authorization is prohibited.
- 23 K. Using the District's wireless equipment while on District property to
24 connect without authorization to any wireless networks other than
25 those provided by the District, is prohibited. External signals will
26 not provide content filtering and access to private networks may be
27 illegal.

28 **Vandalism and Harassment**

29 Vandalism and harassment when utilizing the Internet will result in cancellation of
30 uUser privileges. This includes, but is not limited to, the uploading or creation of
31 computer viruses and the attempt to destroy, harm or modify data of another uUser.

1 **Procedures for Use**

2 Student users must always get permission from their teachers or facilitators before
3 using the nNetwork or accessing any specific file or application. Student users
4 must also follow written and oral classroom instructions.

5 A. All users have the same right to use the computer resources. Users
6 shall not play games without educational value or use the computer
7 resources for non-academic activities when other users require the
8 system for academic purposes
9

10 Personal use of the District nNetwork, including e-mail and the
11 Internet, is permitted as long as it does not interfere with an
12 employee's duties and/or system operation and abides by all District
13 policies and standards.

14 B. Teachers are responsible for teaching proper techniques and
15 standards for participation, for guiding student access to appropriate
16 sections of the Internet, and for assuring that students understand
17 that if they misuse the Network they will lose their privilege to access
18 the Internet from the classroom environment. Students should not
19 be provided with nNetwork access unless they are properly
20 supervised by an individual trained to provide the
21 guidance students require.

22 C. Pursuant to Federal law, students shall receive education about the
23 following:

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

26 2. the dangers inherent with the online disclosure of personally
27 identifiable information; and

28 3. the consequences of unauthorized access (e.g., "hacking"),
29 cyberbullying, and other unlawful or inappropriate activities
30 by students online.
31

32 D. In a Bring Your Own Device (BYOD) school environment, students
33 will be notified of additional responsibilities within the framework of
34 the District's educational objectives. A "device" is defined as "a
35 laptop computer, a smartphone or cellular phone, or any other
36 electronic device that may access the school's network". Staff and
37 students must accept and comply with the following District
38 requirements and restrictions for participation:
39

- 1 1. Users may only connect their devices to the District's filtered
2 Network wirelessly or through a direct connection for data
3 access during school hours, in compliance with the Children's
4 Internet Protection Act (CIPA). Connecting to broadband
5 services for data access during school hours without approval
6 and direction is prohibited. Use of any electronic device, and
7 the telephone capabilities of those devices, are governed by
8 the Codes of Student Conduct (Elementary, Secondary, and
9 Adult).
- 10 2. Users are responsible for ensuring their devices use security
11 applications to protect the devices from infection and prevent
12 spreading infections from the devices.
- 13 3. Users connecting to a school's and/or the District's Network
14 shall release the District from any and all liability for any
15 damage to devices that may or is alleged to have resulted from
16 use of the school's and/or District's Network. The District
17 shall not be responsible for a personally owned device
18 becoming infected when connected to the District's Network
19 or for a student's exposure to inappropriate material when
20 using a personally purchased broadband connection.
- 21 4. The District is not responsible for personally owned devices
22 that are damaged, lost, or stolen.
- 23 5. Pursuant to School Board Policy 5517.01, cyber bullying is
24 prohibited at all times, on campus or off, whether using
25 District-owned equipment and networks or personally owned
26 equipment and broadband connection plans.
- 27 6. Social media like Facebook and similar websites allow Users
28 to "friend" other Users. The District discourages teachers from
29 "friending" students to reduce the possibility of inappropriate
30 communications between them. Students should not try to
31 "friend" teachers. In addition, Users should always be
32 cautious in using social media and, in particular, never reveal
33 personal information about themselves or others.

Inappropriate Material

43 Inappropriate material is material that is inconsistent with the goals, objectives, and
44 policies of the educational mission of the District. It is impossible to control
45 effectively the content of data and an industrious uUser may discover inappropriate
46 material.

Disciplinary Actions for Improper Use

1 The act of ~~accessing the Internet through the~~ using the District's ~~n~~Network signifies
2 that the ~~u~~User will comply with this policy.

3 Disciplinary action for inappropriate use by ~~students~~ Users will be based on the
4 tiered actions described in the Codes of Student Conduct (Elementary, Secondary or
5 Adult) (Policy 5500) and may include, but is not limited to, loss of privilege,
6 suspension or expulsion.

7 F.S. 1001.43, 1001.51
8 H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
9 47 U.S.C. 254(h),(1), Communications Act of 1934, as amended
10 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965,
11 as amended
12 18 U.S.C. 2256
13 18 U.S.C. 1460
14 18 U.S.C. 2246
15 76 F.R. 56295, 56303

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on June 13, 2012, its intention to amend Board Policy, 7540.04, Staff Network and Internet Acceptable Use and Safety, at its meeting on July 18, 2012.

PURPOSE AND EFFECT: The purpose of the proposed Board Policy is to provide the district with a policy containing the standards and guidelines for the responsible use of district network computer systems and the Internet by staff and consequences for failure to abide by these standards.

SUMMARY: The proposed policy changes add language addressing the use of Social Media by staff and the use of personal electronic devices in the coming Bring Your Own Device (BYOD) Wireless Incentive.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING AUTHORITY IS AUTHORIZED: 1001.41 (1) (2); 1001.42 (25); 1001.43 (10) F.S.

LAW IMPLEMENTED, INTERPRETED, OR MADE SPECIFIC: 1001.41; 1001.43; 1001.51; H.R. 4577, 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; 18 U.S.C. 2256; 18 U.S.C. 1460; 18 U.S.C. 2246; 76 F.R. 56295, 56303

IF REQUESTED, A HEARING WILL BE HELD DURING THE BOARD MEETING OF July 18, 2012 which begins at 1:00 p.m. in the School Board Auditorium, 1450 N.E. Second Ave., Miami, Florida, 33132. Persons requesting such a hearing or who wish to provide information regarding the statement of estimated regulatory costs, or to provide information regarding the statement of estimated regulatory costs, or to provide a proposal for a lower regulatory alternative as provided by Section 120.541(1), Florida Statutes, must do so in writing by July 10, 2012, to the Superintendent of Schools, Room 912, at the same address.

ANY PERSON WHO WISHES 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).

A COPY OF THE PROPOSED AMENDED Policy is 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.

Originator: Dr. Richard Hinds
Date: May 30, 2012

1 STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

2 This policy establishes the responsible and acceptable use of the network as a tool
3 for learning in the District. The District Network is defined as all computer
4 resources, including software, hardware, lines and services that allow connection of
5 District computers to other computers, whether they are within the District or
6 external to the District. This includes connection to the Internet while on school
7 property. Users are defined as anyone authorized by administration to use the
8 Network. This includes, but is not limited to, staff, students, parents, vendors,
9 contractors, and volunteers. No User may use the Network to take any action or
10 receive and/or communicate any language that the employee or student could not
11 take or communicate in person. ~~Users are defined as anyone authorized by~~
12 ~~administration to use the Network. This includes, but is not limited to, staff,~~
13 ~~students, parents, vendors, contractors, and volunteers.~~ Prohibitions in applicable
14 Federal, State, and/or local law or regulation, collective bargaining agreements and
15 Board policies are included. Additionally, there is no expectation of privacy in the
16 use of e-mail or network communications when such communications occur over
17 District provided equipment by District employees, students, or others. (See Board
18 policies concerning privacy and e-mail).

19 **Access to the Network**

20 The District Networks gives schools the ability to share educational and research
21 resources from around the world with all students. These resources include access
22 to instructional applications, interactive collaboration between teachers, students
23 and other Users, document sharing, communications of all forms with people from
24 around the world and libraries, museums and research facilities.

1 **Acceptable Use**

2 Use of the ~~an~~Network must support and be consistent with the educational objectives
3 of the District. All ~~u~~Users must comply with this policy and the standards of
4 conduct established in the Codes of Student Conduct (Elementary, Secondary, and
5 Adult), (Policy 550), Florida Code of Ethics of the Education Profession, the District
6 ~~an~~Network Security Standards and policies governing employee behavior.

7 A. Transmission of any material in violation of local, State, and Federal
8 law or regulation or Board policies is prohibited. This includes, but
9 is not limited to copyrighted or trade secret material which the
10 transmitter does not have the right to transmit, and material that is
11 threatening, bullying, discriminatory, slanderous or obscene
12 material ~~or material protected by trade secret.~~

13
14 Obscene material is material which:

- 15 1. the average person, applying contemporary community
16 standards, would find, taken as a whole, appeals solely to the
17 prurient interest; and
- 18 2. depicts or describes, in a patently offensive way, sexual
19 conduct as defined in State law (F.S. 847.001 (11)); and
- 20 3. taken as a whole, lacks serious literary, artistic, political, or
21 scientific value.

22 B. Procedures for protesting instructional materials and educational
23 media as they are accessed through the Internet are governed by
24 Policy 2510.

25 C. The use of the Internet for political activities is prohibited.

26 D. Use of the ~~an~~Network for product advertisement, commercial
27 activities, political campaigning or solicitation is prohibited.

1 E. The District shall use an Internet Content Filter to prevent user
2 access to prohibited material.
3

4 Users of the District's Network are charged with notice that besides
5 obscene material, there are other potentially objectionable materials
6 available on the Internet, including sites with adult content, nudity,
7 and gambling, as well as sites advocating violence and illegal
8 activities. No content filter will ever be 100% accurate, and on
9 occasion either objectionable material may get through or non-
10 objectionable material may be blocked. It is a User's obligation to
11 immediately report these lapses.
12

13 Bypassing the District content filter without authorization is strictly
14 prohibited. The District has procedures in place to evaluate
15 requests from Users to block or unblock sites as necessary.
16

17 Students, parents and staff should be aware that connection to any
18 Internet or network provider not under District control may be
19 unfiltered, especially open wireless connections. The District is not
20 responsible for unfiltered content that may be viewed or downloaded
21 on District equipment that has been provided to individuals for use
22 outside District property. The District is also not responsible for
23 issues caused by the connection of personal devices to the District's
24 Network or improper use of the District's Network or equipment.

25 **Privilege**

26 Accessing the Internet ~~through~~ using District equipment and/or through the
27 District's Network is a privilege, not a right, and inappropriate use, including
28 violation of this rule may result in cancellation of the privilege.

29 A. School, regional center, and District administrators are authorized
30 to determine appropriate and acceptable use pursuant to this policy.

31 B. Any User account may be closed, suspended or revoked at any
32 time a school, regional center, or District administrator determines
33 an account User or holder has used the Network in an
34 inappropriate or unacceptable manner in violation of this or any
35 other applicable District rule.

1 C. Inappropriate or unacceptable use is defined as use that violates
2 this policy or the District's purpose in providing students and
3 employees safe access to the Internet and use that violates the
4 District's Codes of Student Conduct (Elementary, Secondary, and
5 Adult), Florida's Code of Ethics of the Education Profession, the
6 District's nNetwork Security Standards, all Board policies governing
7 employee behavior or any local, State, or Federal law or regulation.

8 D. Access to the Internet from the District nNetwork as a tool for
9 learning will be automatic. Parents must notify the school in writing
10 if they do not want their child to access the Internet.

11 **Monitoring**

12 ~~Administration~~ District staff has the right to review any material on nUser accounts
13 to maintain adequate fileserver space and monitoring appropriateness of material
14 accessed transmitted through the nNetwork. The District shall respect the privacy
15 rights of nUser accounts unless there is a violation of this policy.

16 **Network Etiquette**

17 All nUsers are expected to follow the generally accepted rules of network etiquette.
18 These standards of conduct include, but are not limited to the following:

19 A. Users should be polite. The use of abusive language is prohibited.

20 B. Use appropriate language. The use of profanity, vulgarities or any
21 other inappropriate language is prohibited.

22 C. Engaging in activities which are prohibited under local, State, or
23 Federal law is prohibited.

24 D. Activities which violate the Code of Student Conduct (both
25 elementary and secondary), Code of Conduct for Adult Students, the
26 Code of Ethics of the Education Profession in the State of Florida,
27 the District's nNetwork Security Standards and policies governing
28 employee behavior are prohibited.

29 E. Do not reveal your personal address and/or telephone number or
30 that of other nUsers unless compelled to by law.

1 F. Electronic mail (e-mail) is not guaranteed to be private. People who
2 operate the system do have access to all mail. Messages relating to
3 or in support of illegal activities will be reported to the authorities
4 without notice.

5
6 G. Do not use the nNetwork in such a way that other uUsers would be
7 unable to get the full benefit of information available. This includes,
8 but is not limited to: running applications that deny the nNetwork's
9 services to others, tying up computers without a legitimate
10 educational or School District or school business purpose while
11 others are waiting, damaging software or hardware so that others
12 are unable to use it, or any conduct that would be prohibited by
13 State law (F.S. 815.06).

14 H. Do not use the nNetwork to send or receive messages that
15 discriminate based on sex, race, color, religion, ethnic or national
16 origin, political beliefs, marital status, age, sexual orientation,
17 gender, gender identity, social and family background, linguistic
18 preference, disability or that are inflammatory.

19 **Services**

20 Use of any information obtained via the Internet is at the uUser's own risk. The
21 District will not be responsible for any damages a uUser may incur. This includes,
22 but is not limited to, loss of data resulting from delays, non-deliveries, mis-
23 deliveries, or service interruptions caused by negligence, errors, or omissions.

24 The District is not responsible for the accuracy or quality of information obtained
25 through the nNetwork. All uUsers need to consider the source of any information
26 they obtain through the nNetwork, and evaluate the accuracy of the information.

27 **Security**

28 Security on any computer nNetwork is a high priority, especially when the system
29 involves many uUsers.

30 A. If a uUser can identify a security problem on the nNetwork, the
31 uUser must notify a system administrator. The uUser must not
32 disclose or demonstrate the problem to others.

33 B. Users must not use another individual's account without written
34 permission from that individual. Attempts to log into the system as
35 any other uUser will result in disciplinary action as described in
36 Disciplinary Action.

- 1 C. Any uUser that has been determined by administrators to have
2 violated this rule may be denied future access to the Internet
3 through the District nNetwork.
4
- 5 D. A uUser with a history of using other computer systems in an
6 inappropriate or unacceptable manner may be denied access to the
7 District nNetwork.
- 8 E. Users of the nNetwork will be held responsible for all activity
9 associated with the uUser's account. Users should not share their
10 passwords with anyone, engage in activities that would reveal
11 anyone's password or allow anyone to use a computer to which they
12 are logged on.
- 13 F. Accessing chat rooms or instant messaging while using the District's
14 nNetwork is prohibited.
- 15 G. The use of Internet tools such as blogs and discussion boards are
16 intended for educational purposes only.
- 17 H. Downloading pictures, sounds, video clips, text documents or any
18 material without authorization and without confirmation is
19 prohibited unless that the material is not copyrighted is prohibited.
20 User has the right to use it or has obtained permission from the
21 copyright owner.
- 22 I. Downloading games, video files, audio files or running streaming
23 media without educational value and without authorization by a
24 teacher or a local administrator is prohibited. These applications tie
25 up a great deal of bandwidth and storage and many of the files
26 infringe on the owners' copyrights.
- 27 J. Uploading, Downloading or installing software applications without
28 authorization is prohibited.
- 29 K. Using the District's wireless equipment while on District property to
30 connect without authorization to any wireless networks other than
31 those provided by the District is prohibited. External signals will
32 not provide content filtering and access to private networks may be
33 illegal.

34 **Vandalism and Harassment**

35 Vandalism and harassment when utilizing the Internet will result in cancellation of
36 user privileges. This includes, but is not limited to, the uploading or creation of
37 computer viruses and the attempt to destroy, harm or modify data of another uUser.

1 **Procedures for Use**

2 A. All uUsers have the same right to use the computer resources.
3 Users shall not play games without educational value or use the
4 computer resources for non-academic activities when other uUsers
5 require the system for academic purposes.
6

7 Personal use of the District's nNetwork, including e-mail and the
8 Internet, is permitted as long as it does not interfere with an
9 employee's duties, a student's learning activities and/or system
10 operation and abides by all district policies and standards, State
11 and Federal statutes, and codes of conduct. This use is a privilege,
12 not a right, and any unacceptable use may be subject to appropriate
13 disciplinary action, up to and including dismissal from employment.

14 B. Teachers are responsible for teaching proper techniques and
15 standards for participation, for guiding student access to
16 appropriate sections of the Internet, and for assuring that students
17 understand that if they misuse the nNetwork they will lose their
18 privilege to access the Internet from the classroom environment.
19 Students should not be provided with network access unless they
20 are properly supervised by an individual trained to provide the
21 guidance students require.

22 C. Blogging is the activity of writing entries in, adding material to, or
23 maintaining a "weblog." Employees shall not engage in blogging
24 activities during working hours or use District-owned equipment
25 unless they are specifically required to perform the employees'
26 responsibilities and duties. District uUsers are reminded that
27 during non-working hours they are representatives of the District
28 and should behave in a manner that does not disrespect or discredit
29 the education profession. Unless engaging an officially sanctioned
30 District activity, employees using "blogs" should clearly specify that
31 any opinions or statements are the employee's and do not reflect the
32 views of the District. Employees are prohibited from using officially
33 sanctioned School District logos, school mascots, and other official
34 symbols.
35

36 D. In a Bring Your Own Device (BYOD) school environment, staff must
37 notify students of the additional responsibilities within the
38 framework of the District's educational objectives. A "device" is
39 defined as "a laptop computer, a smartphone or cellular phone, or
40 any other electronic device that may access the school's Network".
41 Staff and students must accept and comply with the following
42 District requirements and restrictions for participation:

- 1
2 1. Users may only connect personally owned devices to the
3 District's filtered Network wirelessly or through a direct
4 connection for data access during instructional time.
5 Connecting to broadband services is prohibited unless there
6 is a specific instructional purpose for doing so. Teachers
7 should instruct students to only connect their devices to the
8 District's filtered wireless Network for data access during
9 school hours.
- 10
11 2. Users are responsible for ensuring their devices use security
12 applications to protect the devices from infection and prevent
13 spreading infections from the devices.
- 14
15 3. Users connecting to a school's and/or District's Network shall
16 release the District from any and all liability for any damage
17 to devices that may or is alleged to have resulted from use of
18 the school's and/or District's network. The District shall not
19 be responsible for a personally owned device becoming
20 infected when connected to the District's Network.
- 21
22 4. Pursuant to School Board Policy 5517.01, cyber bullying is
23 prohibited at all times, on campus or off, whether using
24 District-owned equipment and networks or personally owned
25 equipment and broadband connections.
- 26
27 5. An employee's personal or private use of social media, such as
28 Facebook, Twitter, MySpace, blogs, etc, may have unintended
29 consequences. Employee's may not post material of any
30 nature that violates School Board policies involving employee
31 conduct, state or federal law, or that disrupts the school
32 environment. In addition, as in all other forms of contact
33 between staff and students, inappropriate personal
34 communications using social media is prohibited. If
35 inappropriate contact is found to have occurred, appropriate
36 disciplinary action will be taken. This prohibited conduct
37 applies to staff members' online conduct that occurs off
38 school property including from the employee's private
39 computer. Postings to social media should be done in a
40 manner that reflects credit upon the employee and the school
41 system, is sensitive to the staff member's professional
42 responsibilities and does not violate the Principles of
43 Professional Conduct for the Education Profession in Florida
44 and the Code of Ethics of the Education Profession in Florida.

45
46 Social media sites allow Users to become a "friend" or
47 otherwise associate their "profiles" in a more private and
48 personal arrangement which may mask inappropriate

1 contact. Because the BYOD program is intended to expand
2 the educational tools available to educators, staff are
3 discouraged from "friending" students on Facebook or other
4 similar websites.

5
6 In addition, pursuant to federal and state confidentiality laws,
7 staff are not permitted to use or disclose personally
8 identifiable student information and information contained in
9 student education records without parental consent. See
10 Policy 8330. Staff members also may not disclose or post
11 confidential employee information.

12
13 Staff members may use non-District social media for collective
14 bargaining purposes and union organizational activities.

15
16 D. E. Staff members will participate in professional development programs
17 that include:

- 18 1. the safety and security of students while using e-mail, chat
19 rooms, social media, and other forms of electronic
20 communications;
- 21 2. the inherent danger of students disclosing personally
22 identifiable information online; and
- 23 3. the consequences of unauthorized access (e.g., "hacking"),
24 cyberbullying, and other unlawful or inappropriate activities
25 by students or staff online.

26 Staff members shall provide instruction for their students regarding the appropriate
27 use of technology and online safety and security as specified above.

28 The disclosure of personally identifiable information about students online or via
29 any other method is prohibited.
30
31

32
33 **Inappropriate Material**

34 Inappropriate material is material that is inconsistent with the goals, objectives and
35 policies of the educational mission of the District. It is impossible to control
36 effectively the content of data and an industrious user may discover inappropriate
37 material.

38 **Disciplinary Action**

1 The act of ~~accessing the Internet through the~~ using the District's ~~n~~Network signifies
2 that the ~~u~~User will comply with this policy.

3 Disciplinary action for inappropriate use by ~~staff~~ Users will be taken pursuant to the
4 applicable collective bargaining agreements.

- 5 F.S. 1001.41
6 H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
7 47 U.S.C. 254(h),(1), Communications Act of 1934, as amended
8 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965,
9 as amended
10 18 U.S.C. 2256
11 18 U.S.C. 1460
12 18 U.S.C. 2246
13 76 F.R. 56295, 56303