Office of Superintendent of Schools
Board Meeting of June 13, 2012

May 30, 2012

Financial Services
Richard H. Hinds, Chief Financial Officer

SUBJECT: **PROPOSED AMENDMENT OF BOARD POLICIES: INITIAL 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

This item is submitted for consideration by the Board 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. It also includes a revision of the title to "Responsible Use" to better reflect that students will have additional responsibilities as well as additional benefits in the BYOD environment.

In addition, consideration by the Board is requested 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. It also includes a revision of the title to "Responsible Use" to better reflect that staff will have additional responsibilities as well as additional benefits in the BYOD environment.

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

Authorization of the Board is requested for the Superintendent to initiate rulemaking proceedings in accordance with the Administrative Procedure Act to amend 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.

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 Policy 7540.03, Student Network and Internet Acceptable Use and Safety and Board Policy 7540.04, Staff Network and Internet Acceptable Use and Safety.

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. The word Acceptable in the title is also changed to Responsible to reflect the greater responsibility users must show in the BYOD environment.

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

STAFF NETWORK AND INTERNET RESPONSIBLE ~~ACCEPTABLE~~ USE AND SAFETY

This policy establishes the responsible and acceptable use of the network as a tool for learning in the District. The District network is defined as all computer resources, including software, hardware, lines and services that allow connection of District computers to other computers, whether they are within the District or external to the District. This includes connection to the Internet while on school property. No user may use the network to take any action or receive and/or communicate any language that the employee or student could not take or communicate in person. Users are defined as anyone authorized by administration to use the Network. This includes, but is not limited to, staff, students, parents, vendors, contractors, and volunteers. 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 employees, students, or others. (See Board policies concerning privacy and e-mail).

Access to the Network

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

© MIAMI-DADE 2010

Acceptable Use

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

A. Transmission of any material in violation of local, State, and Federal law or regulation is prohibited. This includes, but is not limited to copyright material, threatening or obscene material or material protected by trade secret.

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.

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

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

D. Use of the network for product advertisement, commercial activities, political campaigning or solicitation is prohibited.

© MIAMI-DADE 2010

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

Users of the District network are charged with notice that besides obscene material, there are other potentially objectionable materials available on the Internet, including sites with adult content, nudity, and gambling, as well as sites advocating violence and illegal activities. No content filter will ever be 100% accurate, and on occasion either objectionable material may get through or non-objectionable material may be blocked.

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

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

Privilege

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

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

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

© MIAMI-DADE 2010

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

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

Monitoring

~~Administration~~ District staff has the right to review any material on user accounts to maintain adequate fileserver space and monitoring appropriateness of material ~~accessed~~ transmitted through the network. The District shall respect the privacy rights of user accounts unless there is possible inappropriate use as described elsewhere in this policy.

Network Etiquette

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

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

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

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

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

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

F. Electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities.

© MIAMI-DADE 2010

G. Do not use the network in such a way that other users would be unable to get the full benefit of information available. This includes, but is not limited to: running applications that deny the network's services to others, tying up computers without a legitimate educational or School 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).

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

Services

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

The District is not responsible for the accuracy or quality of information obtained through the network. All users need to consider the source of any information they obtain through the network, and evaluate the accuracy of the information.

Security

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

A. If a user can identify a security problem on the network, the user must notify a system administrator. The user must not demonstrate the problem to others.

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

C. Any user that has been determined by administrators to have violated this rule may be denied future access to the Internet through the District network.

© MIAMI-DADE 2010

D. A user with a history of using other computer systems in an inappropriate or unacceptable manner may be denied access to the District network.

E. Users of the network will be held responsible for all activity associated with the user's account. Users should not share their passwords with anyone, engage in activities that would reveal anyone's password or allow anyone to use a computer to which they are logged on.

F. Accessing chat rooms or instant messaging while using the District's network is prohibited.

G. The use of Internet tools such as blogs and discussion boards are intended for educational purposes only.

H. Downloading pictures, sounds, video clips, text documents or any material without authorization and without confirmation that the material is not copyrighted is prohibited.

I. Downloading games, video files, audio files or running streaming media without educational value and without authorization by a teacher or a local administrator is prohibited. These applications tie up a great deal of bandwidth and storage and many of the files infringe on the owners' copyrights.

J. Downloading or installing software applications without authorization is prohibited.

K. 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.

Vandalism and Harassment

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

© MIAMI-DADE 2010

Procedures for Use

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

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 abides by all district policies and standards, State and Federal statutes, and codes of conduct. This use is a privilege, not a right, and any unacceptable use may be subject to appropriate disciplinary action, up to and including dismissal from employment.

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

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

D. In a Bring Your Own Device (BYOD) school environment, staff must notify students of their additional responsibilities within the framework of the District's educational objectives. Staff and students participating in said environment must accept District requirements and restrictions for participation. A "device" is defined as "a laptop computer, a smartphone or cellular phone, or any other electronic device that may access the school's network". The

© MIAMI-DADE 2010

following procedures must be complied with when implementing this policy:

1. Staff will only connect personally owned devices to the District's filtered wireless network for data access during instructional time. Connecting to broadband services is prohibited unless there is a specific instructional purpose for doing so. Teachers should instruct students to only connect their devices to the District's filtered wireless network for data access during school hours.

2. Users must be responsible for ensuring their devices use security applications to protect these devices from infection and to protect the rest of the network's users and resources from the spread of infections from their devices.

3. Users connecting to a school's and/or District's network must release the District from any and all liability for any alleged damage to their devices that may or is alleged to have resulted from their use of the school's and/or District's network. The District cannot be held responsible if a personally owned device becomes infected when connected to the District's network.

4. Cyber bullying is prohibited at all times, on campus or off, whether it is done using District-owned equipment and networks or personally owned equipment and broadband connections. Refer to the District's Policy Against Bullying and Harassment for more details.

5. An employee's personal or private use of social media, such as Facebook, Twitter, MySpace, blogs, etc, may have unintended consequences. Employee's may not post material of any nature that violates School Board policies involving employee conduct, that violate state or federal law, or that disrupts the school environment. In addition, as in all other forms of contact between staff and students, inappropriate personal communications between them using social media is prohibited. If inappropriate contact is found to have occurred, appropriate disciplinary action will take place. This prohibited conduct applies to staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner that reflects credit upon the employee and the school system and that is sensitive to the staff member's professional responsibilities and does not violate the Principles of Professional Conduct for the Education

© MIAMI-DADE 2010

Profession in Florida and the Code of Ethics of the Education Profession in Florida.

Social media sites allow users of those sites to become a "friend" or otherwise associate their "profiles" in a more private and personal arrangement which may mask inappropriate contact. As one of the main components of the BYOD program is to expand the educational tools available to educators, the District therefore discourages staff from "friending" students on Facebook or other similar websites.

In addition, federal and state confidentiality laws forbid schools and their employees from using or disclosing personally identifiable student information and information contained in student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate state and federal confidentiality laws or privacy laws related to the disclosure of confidential employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities when using non-District owned social media.

~~D.~~ E. Staff members will participate in professional development programs that include:

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

2. the inherent danger of students disclosing personally identifiable information online; and

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

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

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

© MIAMI-DADE 2010

Inappropriate Material

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

Disciplinary Action

The act of accessing the Internet through the District's network signifies that the user will comply with this policy.

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

F.S. 1001.41
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

© MIAMI-DADE 2010

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. The word Acceptable in the title is also changed to Responsible to reflect the greater responsibility users must show in the BYOD environment.

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

STUDENT NETWORK AND INTERNET RESPONSIBLE ~~ACCEPTABLE~~ USE AND SAFETY

This policy establishes responsible and acceptable use of the network as a tool for learning in the District. The District network is defined as all computer resources, including software, hardware, lines and services that allow connection of District computers to other computers, whether they are within the District or external to the District. This includes connection to the Internet while on school property. No user may use the network to take any action or receive and/or communicate any language that the employee or student could not take or communicate in person. Users are defined as anyone authorized by administration to use the Network. This includes, but is not limited to, staff, students, parents, vendors, contractors, and volunteers. Prohibitions in applicable Federal, State, and/or local law or regulation, collective bargaining agreements and Board policies are included. Additionally, this policy reflects that 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 employees, students, or others. (See Board policies concerning privacy and e-mail).

Access to the Network

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

©MIAMI-DADE, 2010

Acceptable Use

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

A. Transmission of any material in violation of local, State, and Federal law or regulation or Board policies is prohibited. This includes, but is not limited to copyright material, threatening or obscene material or material protected by trade secret.

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.

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

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

D. Use of the network for product advertisement, commercial activities, political campaigning or solicitation is prohibited.

©MIAMI-DADE, 2010

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

Users of the District network are charged with notice that besides obscene material, there are other potentially objectionable materials available on the Internet, including sites with adult content, nudity, and gambling, as well as sites advocating violence and illegal activities. No content filter will ever be 100% accurate, and on occasion either objectionable material may get through or non-objectionable material may be blocked.

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

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

Privilege

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

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

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

©MIAMI-DADE, 2010

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

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

Monitoring

~~Administration~~ District Staff has the right to review any material on user accounts to maintain adequate fileserver space and monitor appropriateness of material ~~accessed~~ transmitted through the network. The District shall respect the privacy rights of user accounts unless there is possible inappropriate use as described elsewhere in this policy.

Network Etiquette

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

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

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

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

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

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

F. Electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities.

©MIAMI-DADE, 2010

G. Do not use the network in such a way that other users would be unable to get the full benefit of information available. This includes, but is not limited to: running applications that deny the network's services to others, tying up computers without a legitimate educational or school 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).

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

Services

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

The District is not responsible for the accuracy or quality of information obtained through the network. All users need to consider the source of any information they obtain through the network, and evaluate the accuracy of the information.

Security

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

A. If a user can identify a security problem on the network, the user must notify a system administrator. The user must not demonstrate the problem to others.

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

C. Any user that has been determined by administrators to have violated this rule may be denied future access to the Internet through the District network.

©MIAMI-DADE, 2010

D. A user with a history of using other computer systems in an inappropriate or unacceptable manner may be denied access to the District network.

E. Users of the network will be held responsible for all activity associated with the user's account. Users should not share their passwords with anyone, engage in activities that would reveal anyone's password or allow anyone to use a computer to which they are logged on.

F. Accessing chat rooms or instant messaging while using the District network is prohibited.

G. The use of Internet tools such as blogs and discussion boards are intended for educational purposes only.

H. Downloading pictures, sounds, video clips, text documents or any material without authorization and without confirmation that the material is not copyrighted is prohibited.

I. Downloading games, video files, audio files or running streaming media without educational value and without authorization by a teacher or a local administrator is prohibited.

J. Downloading or installing software applications without authorization is prohibited.

K. 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.

Vandalism and Harassment

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

©MIAMI-DADE, 2010

Procedures for Use

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

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

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

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

C. Pursuant to Federal law, 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 with the online disclosure of personally identifiable information; and

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

D. In a Bring Your Own Device (BYOD) school environment, staff must notify students of their additional responsibilities within the framework of the District's educational objectives. Staff and students participating in said environment must accept District requirements and restrictions for participation. A "device" is defined as "a laptop computer, a smartphone or cellular phone, or any other electronic device that may access the school's network". The following procedures must be complied with when implementing this policy:

©MIAMI-DADE, 2010

1. Students will only connect their devices to the District's filtered wireless network for data access during school hours, in compliance with the Children's Internet Protection Act (CIPA). Connecting to broadband services for data access during school hours without approval and direction is prohibited. Use of any electronic device, and the telephone capabilities of those devices, will be as described in the Codes of Student Conduct (Elementary, Secondary, and Adult).

2. Students must be responsible for ensuring their devices use security applications to protect these devices from infection and to protect the rest of the network's users and resources from the spread of infections from their devices.

3. Students connecting to a school's and/or District's network must release the District from any and all liability for any alleged damage to their devices that may or is alleged to have resulted from their use of the school's and/or District's network. The District cannot be held responsible if a personally owned device becomes infected when connected to the District's network. Additionally, the District cannot be held responsible if a student is exposed to inappropriate material when using a personally purchased broadband connection.

4. The District cannot be held responsible for personally owned devices that are damaged, lost, or stolen.

5. Cyber bullying is prohibited at all times, on campus or off, whether it is done using District-owned equipment and networks or personally owned equipment and broadband connection plans. Refer to the District's Policy Against Bullying and Harassment for more details.

6. Social media like Facebook and similar websites allow users to "friend" other users. The District discourages teachers from "friending" students to lessen the possibility of inappropriate communications between them. Students should not try to "friend" teachers. In addition, students should always be cautious in using social media and, in particular, never reveal personal information about themselves or others.

Inappropriate Material

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

©MIAMI-DADE, 2010

Disciplinary Actions for Improper Use

The act of accessing the Internet through the District's network signifies that the user will comply with this policy.

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

F.S. 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

©MIAMI-DADE, 2010