The School Board of Miami-Dade County

Bylaws & Policies

Unless a specific policy has been amended and the date the policy was revised is noted at the bottom of that policy, the Bylaws and Policies of the Miami-Dade County Public Schools were adopted on May 11, 2011 and were in effect beginning July 1, 2011.

7540.03 - STUDENT NETWORK AND INTERNET 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. In this policy, Users are defined as students. No user may use the Network to take any action and/or communicate any language that the employee or student could not take or communicate in person. Prohibitions in applicable Federal, State, and/or local law or regulation, collective bargaining agreements and School 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. (See Board policies concerning privacy and e-mail).

Access to the Network

The District Network gives 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.

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 copyrighted or trade secret material which the transmitter does not have the right to transmit, and material that is threatening, bullying, discriminatory, slanderous or obscene material.

   Obscene material is material which:

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

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.

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. It is a User's obligation to immediately report these lapses.

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 using District equipment and/or through 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.

C. Inappropriate or unacceptable use is defined as use that violates this policy or the District's purpose in providing students and employees safe 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

District Staff has the right to review any material on user accounts to maintain adequate fileserver space and monitor appropriateness of material transmitted through the Network. The District shall respect the privacy rights of user accounts unless there is a violation or suspected violation of 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 without notice.

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 disclose or 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.

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 is prohibited unless the User has the right to use it or has obtained permission from the copyright owner.

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. Uploading, 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.

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, students will be notified of additional responsibilities within the framework of the District's educational objectives. 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". Staff and students must accept and comply with the following District requirements and restrictions for participation:

   1. Users may only connect their devices to the District's filtered Network wirelessly or through a direct connection 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, are governed by the Codes of Student Conduct (Elementary, Secondary, and Adult).
   2. Users are responsible for ensuring their devices use security applications to protect the devices from infection and prevent spreading infections from the devices.
   3. Users connecting to a school's and/or the District's Network shall release the District from any and all liability for any damage to devices that may or is alleged to have resulted from use of the school's and/or District's Network. The District shall not be responsible for a personally

owned device becoming infected when connected to the District's Network or for a student's exposure to inappropriate material when using a personally purchased broadband connection.

4. The District is not responsible for personally owned devices that are damaged, lost, or stolen.
5. Pursuant to Board Policy **5517.01**, cyber bullying is prohibited at all times, on campus or off, whether using District-owned equipment and networks or personally owned equipment and broadband connection plans.
6. Social media like Facebook and similar websites allow Users to "friend" other Users. The District discourages teachers from "friending" students to reduce the possibility of inappropriate communications between them. Students should not try to "friend" teachers. In addition, Users 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.

Disciplinary Actions for Improper Use

The act of using the District's Network signifies that the User will comply with this policy.

Disciplinary action for inappropriate use by Users 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

Revised 7/18/12

©Miami-Dade, 2010