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 RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS

The School Board provides students access to a large variety of technology and network resources which provide multiple opportunities to enhance learning and improve communication within the school district and the community. All users must, however, exercise appropriate and responsible use of school and District technology and information systems. Users include anyone authorized by administration to use the network. This policy is intended to promote the most effective, safe, productive, and instructionally sound uses of network information and communication tools.

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, including connection to the Internet with any device while on school property. The Board shall maintain a system of internet content filtering devices and software controls that meet the Federal standards established in the Children's Internet Protection Act. (CIPA).

Digital Citizen

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

A. respects one's self;

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

B. respects others;

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

C. protects one's self and others;

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

D. respects authorship;

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

E. Protects intellectual property.

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

Responsible Use

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

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

A. Use of the District's network, electronic devices, and social media must be consistent with the District's educational objectives, mission, and curriculum.
B. Transmission of any material in violation of any local, Federal, and State laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material, and defamatory, threatening, offensive, or obscene material.
C. Intentional or unintentional use of District resources to access or process, proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
D. The network may not be used to send or receive messages that discriminate on any protected basis as delineated in the Board's Anti-Discrimination Policy **5517**.
E. Cyberbullying is prohibited at all times, on school grounds or off, whether using District-owned equipment and networks, social media or personally owned equipment and broadband connections of any kind. See Policy **5517.01**, Bullying and Harassment.
F. Software, services, games, applications, video or audio files, or streaming media without educational value may not be installed, uploaded, or downloaded on school devices without prior authorization by a teacher of administrator.
G. Use of District or network resources for commercial activities, product advertisement, religious or political campaigning, lobbying, or solicitation is prohibited.
H. Accessing chat rooms or instant messaging using the District's network is prohibited.
I. Bypassing the District's content filter without authorization is strictly prohibited.
J. Users may not share their passwords and are expected to act with due care in maintaining their passwords private and secure.
K. Users may be held personally and financially responsible for malicious or intentional damage or interruptions to network service, software, data, user accounts, hardware, and/or any other unauthorized use.
L. Files stored on District-managed networks and hardware are the property of the District and may be inspected at any time.
M. Materials published electronically must be for educational purposes. Administrators may monitor these materials to ensure compliance with content standards.

Procedures for Use

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

B. Students shall receive education about the following:

   1. safety and security while using e-mail, chat rooms, social media, and other forms of electronic communications;
   2. the dangers inherent in online disclosure of personally identifiable information; and
   3. the consequences of unauthorized access (e.g., hacking, cyber-bullying, and other unlawful or inappropriate activities online).

C. All student users (and their parents if they are minors) are required to sign a written agreement annually, or at the time of enrollment, to abide by the terms and conditions of this policy and its administrative procedures and guidelines.

D. If authorization has been specifically given by the school for use within the District's educational mission, students may bring their own device such as a laptop computer, a smartphone or cellular phone, or any other device that may access the school or District network. Students and parents must submit a contract for use of the device before being allowed to use it. Students will be notified of any additional responsibilities for use of these devices. The contract must be maintained in the student's cumulative file.

E. Students shall not (1) access or use another person's account without written permission; (2) share their password with anyone else or engage in activities that would reveal anyone's password; (3) allow others to access a computer that the user is logged on to; or (4) ever sign in, or attempt to sign in, as another person.

Social Media

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

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

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

Violations and Sanctions

Accessing the Internet or District network is a privilege, not a right. Inappropriate use and violation of this or any other Board policy may result in cancellation of the privilege. Inappropriate material and use is defined as any material or use that is inconsistent with the goals, objectives, and policies of the educational mission of the District. Any user can be denied access temporarily or permanently if the school, Regional Center, or District administrator determines that a user has used the Internet or District network in an inappropriate or unacceptable manner. Students may also be disciplined pursuant to the applicable *Code of Student Conduct*, Policy 5510. Students may also be subject to other legal action.

Board Liability

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

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

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

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

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

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

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

Administrative Procedures and Guidelines

The Superintendent, or designee, is authorized to develop, implement, and disseminate administrative procedures and user guidelines necessary to effectuate this policy.

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
46 C.F.R. 54.500-54.523

Revised 7/18/12
Revised 6/17/15