Book	Policy Manual
Section	7000 Property
Title	STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS & INTERNET SAFETY
Code	po7540.03
Status	Active
Adopted	May 11, 2011
Last Revised	August 16, 2023

7540.03 - **STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS & INTERNET SAFETY**

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.

I. **District Network & Technology Resources**

The District network is defined as all computer and networked resources, including software, hardware, electronic mail systems, networked devices, cloud storage/solutions, third-party solutions managed by District and/or for which the District has contracted for services, network circuits, 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, regardless of whether it is District/school-issued or personal, 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).

II. **Internet Safety**

The District shall limit student access to the Internet:

A. to only age-appropriate subject matter and materials on the Internet;

B. in a manner that protects the safety and security of students when using e-mail, chat rooms, and other forms of direct electronic communications;

C. in a manner that prohibits access by students to data or information, including so-called "hacking", and other unlawful online activities by students;

D. in a manner that prevents access to websites, web applications, or software that does not protect against the disclosure, use, or dissemination of students' personal information;

E. in a manner that prohibits and prevent students from accessing social media platforms through the use of Internet access provided by the District, except when expressly directed by a teacher or appropriate staff solely for educational or school-related purposes;

F. in a manner that prohibits the use of the TikTok platform or any successor platform on District-owned devices, through Internet access provided by the District, or as a platform to communicate or promote any District school, school-sponsored club, extra-curricular organization, or athletic team.

Any online educational service that students or their parents are required to use must comply with Policy 8330, *Student Information, Records, and Privacy Rights*, F.S. 1006.1494, Student Online Personal Information Protection Act, and all relevant statutes and rules.

III. **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.

IV. **Student Responsible Use**

Responsible use of the District's network 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, their designees, or contracted entities may review files and communications on the District's network and related systems (including but not limited to electronic mail, managed chat applications, and network or cloud storage) 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 on the District's network and related systems which may be subject to disclosure pursuant to Florida's Public Records Act.

Student users shall 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; all users of the District network are bound by the guidelines and stipulations set forth within the Network Security Standards, which are posted on the District's website.

B. Any user who identifies a security problem on the network must notify a system administrator and shall not disclose or demonstrate the problem to others.

C. Students shall not use another individual's account. Users must not share their password with anyone, engage in activities that would reveal anyone's password, or allow others to access a computer that the user is logged on to. Attempting to log in to the system as any other user is prohibited. Students are expected to act with due care in maintaining their passwords private and secure.

D. 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, bullying, discriminating, slanderous, offensive, harassing, cyberstalking, 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.

E. 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.

F. 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.

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

H. 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.

I. Software, services, games, applications, video or audio files, or streaming media without educational value may not be installed, uploaded/downloaded or utilized on District/school devices without prior authorization by a teacher or administrator.

J. Use of District or network resources for commercial activities, product advertisement, and religious or political campaigning, lobbying, or solicitation is prohibited.

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

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

M. 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.

N. Files stored on District-managed networks and hardware are the property of the District and may be monitored or inspected by administrators, their designees, or contracted entities at any time.

O. Materials published electronically must be for educational purposes. Administrators may monitor these materials to ensure compliance with content standards.

V. **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).

4. The social, emotional, and physical effects of social media and any related requirements, as set forth in F.S. 1003.42.

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. A student may possess a wireless communications device while the student is on school property or in attendance at a school function; however, a student may not use a wireless communications device during instructional time, except when expressly directed by a teacher solely for educational purposes. 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. However, teachers shall have authority to designate an area for wireless communications devices during instructional time. The District/school is not responsible if a student's wireless communication or any electronic device is damaged, lost, or stolen. Students will be notified of any additional responsibilities for use of these devices.

E. Students shall be prohibited from utilizing the data access capabilities of a wireless communications device, internet hotspot, or any other connection method that bypasses internet content filtering and/or District security mechanisms to connect to internet-based resources (including, but not limited to social media) during instructional time, unless approved or directed by their teacher and/or other authorized school personnel.

VI. **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 and/or 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.

VII. **Violations and Sanctions**

Inappropriate use and violation of this or any other Board policy may result in suspension of network access and/or discipline in accordance with Policy 5500, Student Conduct and Discipline and the Code of Student Conduct. 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. User access may be affected 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 subject to other legal action.

VIII. **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.

IX. **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.

Effective 07.01.2011
Revised 07.18.2012
Revised 06.17.2015
Revised 03.15.2017
Revised 08.16.2023

Legal

F.S. 748.048

F.S. Ch. 847, et. seq.

F.S. 1001.43

F.S. 1001.51

F.S. 1003.02

F.S. 1003.32

F.S. 1003.42

F.S. 1006.07

F.S. 1006.1494

F.A.C. 6A1.0955

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

20 U.S.C. 6777, 9134 (2003)

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246

47 C.F.R. 54.500, 54.501, 54.502, 54.503, 54.504, 54.505, 54.506, 54.507

47 C.F.R. 54.508, 54.509, 54.511, 54.513, 54.514, 54.515, 54.516, 54.517

47 C.F.R. 54.518, 54.519, 54.520, 54.522, 54.523