Office of Superintendent of Schools
Board Meeting of June 21, 2023

June 8, 2023

Office of the General Counsel
Walter J. Harvey, General Counsel

SUBJECT: **<u>INITIAL</u> READING: PROPOSED AMENDMENTS TO SCHOOL BOARD POLICIES 7540.01, *TECHNOLOGY PRIVACY*, 7540.03, *STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS*, 7540.04, *STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS*, 7540.05, *STAFF ELECTRONIC MAIL*, AND 7540.06, *STUDENT ELECTRONIC MAIL***

COMMITTEE: **ACADEMICS, INNOVATION, EVALUATION, & TECHNOLOGY**

LINK TO STRATEGIC PLAN: **SAFE, HEALTHY, & SUPPORTIVE LEARNING ENVIRONMENTS**

Consistent with the Board's statutory responsibility to periodically review and update policies to conform to legislative changes and District practices, authorization is requested to amend Board Policies 7540.01, *Technology Privacy*, 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*.

Policy 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, is proposed for amendment as a result of HB 379 (2023), amending F.S. 1003.02 to require each district school board to adopt an internet safety policy for student access to the Internet, which limits access by students to only age-appropriate subject matter and materials on the Internet; protects the safety and security of students when using e-mail, chat rooms, and other forms of direct electronic communications; prohibits access by students to data or information, including so-called "hacking," and other unlawful online activities by students; prevents access to websites, web applications, or software that does not protect against the disclosure, use, or dissemination of students' personal information; prohibits and prevents students from accessing social media platforms through the use of Internet access provided by the school district, except when expressly directed by a teacher solely for educational purposes; and prohibits the use of the TikTok platform or any successor platform on district-owned devices, through Internet access provided by the school district, or as a platform to communicate or promote any district school, school-sponsored club, extracurricular organization, or athletic team. Additionally, the bill amends F.S. 1003.32 to grant teachers the

authority to designate an area for wireless communications devices during instructional time.

The policy title is also recommended for revision to include “Internet Safety.”

Additionally, to promote safety throughout the District, the policy is recommended for amendments to clarify expectations for student responsible use and reiterate that administrators, their designees, or contracted entities may review files and communications on the District network and related systems (including 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. Similar amendments are proposed to Policies 7540.01, *Technology Privacy*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*, for the same purposes.

The policy amendments and adoption were drafted in collaboration with, and reviewed by the Superintendent, Cabinet, and the Office of the General Counsel. The Notice of Intended Action and policies with strikethroughs and underlines are attached.

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 Policies 7540.01, *Technology Privacy*, 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*.

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on June 21, 2023, its intention to amend Board Policies 7540.01, *Technology Privacy*, 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*, at its meeting of August 16, 2023.

PURPOSE AND EFFECT: Board Policies 7540.01, *Technology Privacy*, 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*. are proposed for amendment as a result of recent legislation and to promote safety throughout the District.

SUMMARY: Policy 7540.03, *Student Responsible Use of Technology*, *Social Media, and District Network Systems*, is proposed for amendment as a result of HB 379 (2023), amending F.S. 1003.02 to require each district school board to adopt an internet safety policy for student access to the Internet, which limits access by students to only age-appropriate subject matter and materials on the Internet; protects the safety and security of students when using e-mail, chat rooms, and other forms of direct electronic communications; prohibits access by students to data or information, including so-called "hacking," and other unlawful online activities by students; prevents access to websites, web applications, or software that does not protect against the disclosure, use, or dissemination of students' personal information; prohibits and prevents students from accessing social media platforms through the use of Internet access provided by the school district, except when expressly directed by a teacher solely for educational purposes; and prohibits the use of the TikTok platform or any successor platform on district-owned devices, through Internet access provided by the school district, or as a platform to communicate or promote any district school, school-sponsored club, extracurricular organization, or athletic team. Additionally, the bill amends F.S. 1003.32 to grant teachers the authority to designate an area for wireless communications devices during instructional time. The policy title is also recommended for revision to include “Internet Safety.” Additionally, to promote safety throughout the District, the policy is recommended for amendments to clarify expectations for student responsible use and reiterate that administrators, their designees, or contracted entities may review files and communications on the District network and related systems (including 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. Similar amendments are proposed to Policies 7540.01, *Technology Privacy*, 7540.04, *Staff Responsible Use of Technology, Social Media, and District Network Systems*, 7540.05, *Staff Electronic Mail*, and 7540.06, *Student Electronic Mail*, for the same purposes.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: Fla. Stat. ss. 1001.41(1), (2); 1001.42(6), (8); 1001.43(1), (7), (11).

LAWS IMPLEMENTED INTERPRETED OR MADE SPECIFIC: Fla. Stat. ss. F.S. 119.011; 257 et seq.; 668.60 et seq.; 668.701 et seq.; 748.048; Ch. 847; 1003.02; 1003.32; 1006.07(2)(m), (6); 1006.1494; 1012.32; 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; 18 U.S.C. 2256; 18 U.S.C. 1460; 18 U.S.C. 2246; 47 C.F.R., Part 54; F.A.C. 6A-1.0955.

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF August 16, 2023, which begins at 1:00 p.m., in the School Board Auditorium, 1450 N.E. Second Avenue, Miami, Florida 33132. Persons requesting such a hearing or who wish to provide information regarding the statement of estimated regulatory costs, or to provide a proposal for a lower cost regulatory alternative as provided in Section 120.54(1), F.S., must do so in writing by July 19, 2023, to the Superintendent, Room 912, at the same address.

ANY PERSON WHO DECIDES 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)

COPIES OF THE PROPOSED AMENDED POLICY are 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.

Book	Policy Manual
Section	June 21, 2023 - Initial Reading
Title	TECHNOLOGY PRIVACY
Code	7540.01
Status	Initial Reading

7540.01 - **TECHNOLOGY PRIVACY**

All computers, telephone systems, voice mail systems, electronic mail systems~~, and voice mail systems~~ networked devices, cloud storage/solutions, third-party solutions managed by District staff and/or for which M-DCPS has contracted for services are ~~the~~considered District~~'s~~ property and are to be used primarily for business or educational purposes. The District ~~has~~ retains the right to monitor, access and review all networked devices, cloud storage/solutions, third-party solutions managed by District staff and/or for which M-DCPS has contracted for services, electronic and voice mail, computer files, data bases, and any other electronic transmissions contained in or used in conjunction with the District's network computer system, telephone system, electronic mail system, ~~and~~ voice mail system, and any related ancillary systems. Students and ~~S~~staff members should have no expectation that any information on these systems is confidential or private.

Review of such information may be done by, or at the request of, the District with or without the student or staff member's knowledge. Passwords should be kept confidential. The District retains the right to access information in spite of a password. A staff member's refusal to permit such access may be grounds for discipline up to and including discharge.

Computers, network or cloud storage, electronic mail, and voice mail are to be used for business purposes. Personal messages via District-owned technology should be limited according to District regulations. Staff members are encouraged to keep their personal records and personal business at home. In addition, staff members shall be advised that computers, network or cloud storage, electronic mail, and voice mail are subject to Florida's Sunshine Law.

Students and ~~S~~staff members are prohibited from sending, storing, posting or otherwise distributing any threatening, offensive, discriminatory, ~~or~~ harassing, or sexually inappropriate computer, electronic, or voice mail messages and should remain vigilant for potential cyber threats. All ~~employees~~ users have an obligation to ~~should~~ report any suspected cyber threats to the site technician or administrator.

Review and/or monitoring of computer files, network or cloud storage, electronic mail, and voice mail may be performed at any time ~~will only be done in the ordinary course of business~~. If a student or staff member's personal information is discovered, the contents of such discovery will not be reviewed by the District, except to the extent necessary to determine whether there is an imminent safety threat or the District's interests have been compromised. Any information discovered will be limited to those who have a specific need to know that information.

The administrators and supervisory staff members authorized by the Superintendent have the authority to search and access information electronically.

~~All computers and a~~Any information or software on any of the aforementioned systems are ~~the computers are~~ the property of the District. Students and ~~S~~staff members shall not remove or communicate any such information in any form for their personal use or for the use of others. In addition, students and staff members may not copy software on any District computer and may not bring software from outside sources for use on District equipment without the prior approval ~~of the Superintendent~~from Information and Technology Services (ITS), pursuant to Network Security Standards. Such pre-approval ~~will~~ may include a review of any license or copyright infringements, in addition to potential vulnerabilities ~~or virus problems~~ associated with such outside software.

See the District Network Security Standards and Board policies concerning staff and student use of e-mail, and staff and student Network and Internet Acceptable Use for more details.

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.

Effective 07.01.2011
Revised 12.09.2020

Legal References:
F.S. 119.011
F.S. 1001.43
F.S. 1001.51

F.S. 1003.02
F.S. 1006.07
F.S. 1006.1494
F.A.C. 6A-1.0955
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., Ch. I, Subch. B, Pt. 54, Subpt. F

Adoption Date: 05.11.2011

Book	Policy Manual
Section	June 21, 2023 - Initial Reading
Title	STUDENT RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS
Code	7540.03
Status	Initial Reading

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 staff and/or for which M-DCPS has contracted for services, network circuits~~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, 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; and

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 solely for educational 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, extracurricular 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 ~~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, or contracted entities may review files and communications on the District 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 network and related systems which may be subject to disclosure pursuant to Florida's Public Records Act.

Student ~~U~~users ~~are expected to~~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.

~~B.~~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.

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

~~D.~~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*.

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

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

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

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

~~I. Users may not share their passwords and are expected to act with due care in maintaining their passwords private and secure.~~

~~J.~~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.

~~K. Files stored on District-managed networks and hardware are the property of the District and may be inspected at any time.~~

~~L.~~ 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. 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 communication 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 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.~~

~~D.~~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.

~~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.~~

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 ~~or~~ 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

~~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 suspension of network access and/or discipline in accordance with Policy 5500, *Student Conduct and Discipline* and *the Code of Student Conduct* ~~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 u~~User access may be ~~can be denied access temporarily or permanently~~ 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 disciplined pursuant to the applicable *Code of Student Conduct*, Policy 5510~~. 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

Legal References:
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. 6A-1.0955
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

Adoption Date: 05.11.2011

Book	Policy Manual
Section	June 21, 2023 - Initial Reading
Title	STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS
Code	7540.04
Status	Initial Reading

7540.04 - **STAFF RESPONSIBLE USE OF TECHNOLOGY, SOCIAL MEDIA, AND DISTRICT NETWORK SYSTEMS**

The School Board provides 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 are defined as anyone authorized by administration to use the network. This includes, but is not limited to: staff, vendors, contractors, and volunteers. For purposes of this policy, the term "staff" shall include all District employees and non-student users, such as charter school employees, contractors, volunteers. 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 staff and/or for which M-DCPS has contracted for services, network circuits~~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, 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. 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 references including work, websites, books, media, etc., used in the development of any presentations, curriculum, etc.

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.

III. Staff Responsible Use

Responsible use of the District's network ~~technology resources~~ is expected to be ethical, respectful, academically honest, and supportive of the District's educational mission and objectives. 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, or contracted entities may review files and communications (including but not limited to electronic mail, managed chat applications and network or cloud storage) to ensure the system is being used in accordance with District policy and administrative procedures and guidelines. Users do not have any expectation of privacy in files stored on electronically on the District network and related systems~~servers or disks~~ which may be subject to disclosure pursuant to Florida's Public Records Act.

~~No user may~~ All users are expected to 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 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 staff ~~employees~~, students, or others (See Policy 7540.05).

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

A. Use of the District's Network and electronic devices must be consistent with the District's educational objectives, mission, and curriculum; all users of the District's 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. ~~Employees~~ Staff shall not use another individual's account ~~without written permission~~. 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. ~~Employees are~~Staff is expected to act with due care in maintaining their passwords private and secure.

D. Transmission of any material in violation of local, Federal, and/or 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 in any way that discriminates on any protected basis as delineated in the Board's anti-discrimination policies.

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

H. Downloading pictures, sounds, video clips, text documents, or any material without authorization and without confirmation is prohibited unless the employee has the right to use it or has obtained permission from the copyright owner.

I. Downloading games, video files, audio files, or streaming media without educational value or without prior authorization by an administrator is prohibited.

J. Uploading, downloading, transferring, or installing software applications, images, texts, video files, and digital music files without authorization is prohibited.

K. Use of District resources for commercial activities, product advertisement, or religious or political campaigning, lobbying, threats, suggestions of violence, or solicitation is prohibited.

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

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

N. 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.

~~O. Files stored on District-managed networks and hardware are the property of the District and may be inspected at any time.~~

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

~~Q. Materials published electronically must be for educational purposes. Administrators should monitor these materials to ensure compliance with~~

~~content standards.~~

~~R.~~P. Software, services, games, applications, video or audio files, or streaming media obtained without permission may never be installed, uploaded/~~, or~~ downloaded or utilized on District/school devices without prior authorization by Information Technology Services (ITS).

~~S.~~Q. Cyberbullying is prohibited at all times, on campus or off, whether using District-owned equipment and networks or personally owned equipment and broadband connections.

R. 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.

~~T.~~ Files stored on or accessed via District-managed networks and hardware as defined previously in this policy are the property of the District and may be monitored or inspected by administrators, their designees, or contracted entities at any time. Materials published electronically must be for educational purposes. Administrators should monitor these materials to ensure compliance with content standards.

IV. Procedures for Use

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

B. Staff members shall participate in professional development and provide instruction to students that includes:

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

2. the dangers inherent in disclosing personally identifiable information online and/or passwords; and

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

~~3.~~4. The social, emotional, and physical effects of social media and any related requirements, as set forth in F.S. 1003.42.

C. ~~Employees are~~Staff is required to affirm that they have read and agree to comply with this policy on a yearly basis.

D. 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 complies with all District policies and standards, State and/or Federal law, and Florida's Code of Ethics for the Education Profession.

E. Blogging is the activity of writing entries in, adding material to, or maintaining a "weblog". A podcast is an audio show or series available for download or streaming via the internet (similar to a radio show). Employees shall not engage in blogging activities, recording podcasts or engaging in any other similar/related communication forums during working hours or use District-owned equipment for blogging, podcast, or similar/related activities unless specifically stated in their responsibilities and duties. During non-working hours, staff members are representatives of the District and should behave in a manner that does not disrespect or discredit the education profession. Unless engaging in an officially sanctioned District activity, employees using "blogs," podcasts, and/or similar communication forums should clearly specify that any opinions or statements are the employee's own and do not reflect the views of the District. ~~Employees are~~Staff is prohibited from using School District logos, school mascots, and other official symbols.

F. ~~Employees are~~Staff is not permitted to use or disclose personally identifiable student information and information contained in student education records without parental consent (See Policy 8330). Staff members may not disclose or post confidential employee information.

V. 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 school(s).

Board members, the District offices, and schools are permitted to create social media accounts, in compliance with District guidelines, to share District and school 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, staff shall comply with the same responsible use rules outlined above for Internet and District network use. In addition, students and staff 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. The use of District time and/or equipment for personal social media activities is prohibited. Students and staff may be disciplined by the District for inappropriate social media

behavior, even if it occurs off campus. Inappropriate personal communications using social media is prohibited.

Some social media sites allow users to become a "friend" or otherwise associate their "profiles" in a more private and personal arrangement which may mask inappropriate conduct. Staff members are discouraged from "friending" students on Facebook or other similar websites/applications, other than for the limited purpose of communications necessary to further educational objectives.

Employees shall not use District or school social media for collective bargaining purposes or union organizational activities~~,~~ but may use non-District social media for these purposes.

The District shall prohibit 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, extracurricular organization, or athletic team.

VI. 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 suspension of network access and/or employee discipline ~~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, Region, or District administrator determines that a user has used the Internet or District network in an inappropriate or unacceptable manner. Staff may be disciplined or subject to legal action for violations of this policy.

VII. Board Liability

The Board is not responsible for, and cannot be held liable for:

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

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

C. use of any 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, or omissions;

D. the accuracy or quality of information obtained through the network;

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

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

VIII. 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.

IX. Training

Annual training on cybersecurity will be conducted for District employees.

Effective 07.01.2011
Revised 07.18.2012
Revised 06.17.2015
Revised 03.15.2017
Revised 12.09.2020

Legal References:
F.S. 748.048
F.S. 847, et. seq. ~~.012,~~
F.S. 1001.41~~,~~
F.S. 1012.32
P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h),(1), Communications Act of 1934, as amended (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
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

Adoption Date: 05.11.2011

Book	Policy Manual
Section	June 21, 2023 - Initial Reading
Title	STAFF ELECTRONIC MAIL
Code	7540.05
Status	Initial Reading

7540.05 - **STAFF ELECTRONIC MAIL**

This policy establishes the use of the District's electronic email (e-mail) system designated for use by staff and other District- authorized users and applies to any and all electronic messages composed, sent, or received by any authorized District user. Authorized users of e-mail are employees, temporary or contract employees, elected School Board members and their staff, and any other individuals or groups issued District staff e-mail accounts. (See also Policy 7540.04)

I. District E-Mail

E-mail is an official means of communication within the District. The use of e-mail is encouraged as a convenient, timely, and cost-effective communications medium. The purpose of providing an e-mail system to District employees is to advance the Board's business needs, mission, and goals. Employees who use the District e-mail services are expected to do so responsibly and to comply with Florida and Federal laws, District policies and procedures, and established standards of professional conduct and personal courtesy.

II. Acceptable Use of District E-mail Services

Use of District e-mail by employees must support and be consistent with District objectives. All users must be aware of and understand the standards by which the District expects and requires users to conduct themselves. These standards are found in, among other things, the Code of Ethics for the Education Profession in the State of Florida, the Principles of Professional Conduct for the Education Profession

in Florida, the District's Electronic-Handbook, Policy 7540.04, and the District's Network Security Standards. All users must familiarize themselves with all applicable standards. An employee's failure to become familiar with these guidelines will not constitute a viable defense to or be a mitigating factor to a charge that an employee has violated this policy.

III. Unacceptable Use of District E-mail Services

Authorized users of the e-mail system may not use the District's e-mail system to perform any action or transmit any communication that would otherwise be prohibited in any other medium of communication.

Unacceptable and prohibited uses of District e-mail services include, but are not limited to:

A. Using profanity, obscenity, or other language which may be offensive to another user or any matter deemed to be obscene.

   Obscene material is material which: 1) the average person, applying contemporary community standards, would find, taken as a whole appeals to prurient interests; 2) depicts or describes in a patently offensive way, sexual conduct as defined by state law; 3) or taken as a whole lacks serious literary, artistic, political, or scientific value.

B. Transmitting any material that is in violation of Federal, State, and local laws, or of Board policies, regulations, or guidelines. This includes, but is not limited to, material that is obscene, pornographic, or contains statements that would violate an individual's civil or constitutional rights or constitute bullying, harassment, slander, defamation, discrimination, cyberstalking, or trade secrets or copyrighted material without the consent of the owner or copyright holder. (See also Policy 7540.04)

C. "Spoofing" where spoofing is defined as the act of disguising the sender of an e-mail by replacing the name in the "from" or header fields, sending e-mails while signed on as a different user, or otherwise intentionally misleading the recipient as to the identity of the actual sender.

D. Sending anonymous e-mail.

E. Engaging in any activity designed to view the e-mails of other individuals without authority or permission.

F. Using the District's global distribution lists for purposes that are not work related.

G. Initiating or forwarding "chain-letters" or petitions.

H. Using the e-mail system for political activities. Board Policies~~y~~ 1232, ~~Policy~~ 3232, and ~~Policy~~ 4232, *Political Activities*, govern the political activities of employees while on duty. In addition, all authorized users are prohibited from using the District's e-mail system to provide publicity for any candidate for public office, and are forbidden from using the District's private network for lobbying, campaigning, or soliciting on behalf of any candidate for public office or using e-mail to support or oppose a political or union position or to engage in political or union activity. This includes sending messages regarding these topics into the District's e-mail system from an external e-mail account.

I. "Spamming," or the sending of unwanted, unsolicited and/or unnecessary messages to large numbers of people, usually with the purpose of advertising a product, event, service, or lobbying for a specific political position or promoting an individual's opinion. In many cases, the sender is unknown to the recipients. The District has the right to block and/or remove any e-mail that it determines is spam.

J. Violating Board policies, including, but not limited to, Florida's Code of Ethics of the Education Profession, The Principles of Professional Conduct for the Education Profession in Florida, and Board Policy 1210, Policy 3210, and Policy 4210. Board members and employees are expected to prevent any entity from sending political e-mail into the District e-mail system in the Board or employee's name.

IV. Consequences of Inappropriate Use of District E-mail Services

The e-mail system is the property of the District. The District has the right to monitor the e-mail system for unacceptable use according to Federal, State, local and District laws, policies and rules. Any employee who violates this rule is subject to appropriate disciplinary action, up to and including dismissal.

A. Work-site supervisors and District administrators are authorized to determine whether an employee is in compliance with this rule and is using the District's e-mail system in an appropriate and acceptable manner. This includes randomly accessing the employee's e-mail for the purpose of determining compliance with this rule.

B. The District also has the right to:

1. review e-mails stored in the District email system~~network~~ for the purpose of maintaining adequate and necessary ~~file server~~ storage space, to determine whether there is an imminent safety threat or the District's interests have been compromised, and to ensure appropriate use and compliance with Policies 7540.01, *Technology Privacy*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Security Systems & Internet Safety*,

2. modify or delete e-mails or attachments that may contain computer viruses or any other computer code that could damage or destroy any portion of the network, and

3. block e-mails that violate this policy.

C. Users of the District e-mail system shall not expect that e-mail generated or received via the District's e-mail system will remain private. Users should be aware that:

1. Sensitive and confidential data, including data considered exempt from public disclosure, may be viewed by persons other than the intended recipient. Information that is exempt or confidential under state and federal law may need to be encrypted, blocked out, or not transmitted by e-mail.

2. E-mail is legally discoverable and may be used in court proceedings. Employees are notified that there is no individual right to privacy in the use of the District's e-mail system. Administration has an absolute right to monitor employees' use of the e-mail system at its discretion. Users are warned that although e-mail often has the feel of a private conversation, it is in fact, not private. Further, e-mail generated during the regular course of School Board business is subject to public disclosure, in accordance with Florida's Public Records Act, F.S. Chapter 119.

V. Personal Use of District E-mail Services

The intended use of the District e-mail system is for District-related purposes, not for personal use or other purposes. In limited instances, some personal use of the District e-mail system may be permitted. This use is a privilege, not a right. Limited, incidental personal use of the District e-mail system such as sending short, brief e-mails to a friend or relative is permissible so long as the user complies with the Utilization Policy and with State and Federal laws and Board policies governing the use of e-mail. Any abuse of this privilege will be handled in the same manner as described above.

Limited incidental personal use must not tie-up or otherwise obstruct system resources in any way, interfere with an individual's job performance and/or duties, advertise or promote a product or service, publicize unsanctioned, non-District activities without approval, promote political candidates or positions as outlined above, include attachments that use excessive storage (multiple pictures, video clips, etc.), and/or be used in any way that is detrimental to the District. In addition, employees are prohibited from storing e-mail that is personal in nature in the District's e-mail system.

The above list is for illustrative purposes only and is not exhaustive. Employees must exercise good judgment in using the e-mail system and not abuse the privilege.

VI. Retention

All Federal, State, and local rules and regulations regarding retention of records, memos, and documents apply to documents and materials created and transmitted by e-mail. F.S. Chapter 257 establishes the authority of the Division of Library and Information Services, Department of State, to establish and maintain the standards and guidelines for public records.

Users of District e-mail are responsible for retaining e-mail that, by law, must be retained according to the minimum retention periods set by the Florida Department of State General Records Schedule GS7. If a public record is maintained longer than required, it remains a public record and must be produced upon request. Upon termination of employment, individuals are required by law to provide their employer with, and/or leave intact, any record (including e-mail) subject to the retention laws and schedules. Violators may be subject to personal and/or criminal liability. Official District business should not be conducted via personal e-mail accounts and/or text messaging, but rather via District-issued e-mail accounts.

E-mail that should be retained may be stored electronically or printed and saved as a hard-copy, provided that printed copies maintain all applicable routing information (e.g., to/from information) along with date/time stamps. In either case, such records must be available for public access, regardless of the medium in which they are maintained. The State and the courts do acknowledge, however, that much of what is put in e-mail does not qualify as a public record and may be deleted without permission once it no longer has value. Users must consult the GS7 schedule for required retention periods, exemptions, and other factors that may influence the disposition and/or disposal of public records.

Updated retention schedule information can be found at the following link: http://dos.myflorida.com/library-archives/records- management/general-records-schedules/.

Effective 07.01.2011
Revised 03.15.2017

Legal References:
F.S. 119.011
F.S. 257 et seq.
F.S. 257.05
F.S. 668.60 et seq.
F.S. 668.701 et seq.
F.S. 748.048

F.S. Ch. 847, et. seq. ~~.012~~

Adoption Date: 05.11.2011

Book	Policy Manual
Section	June 21, 2023 - Initial Reading
Title	STUDENT ELECTRONIC MAIL
Code	7540.06
Status	Initial Reading

7540.06 - **STUDENT ELECTRONIC MAIL**

This policy establishes the use of District student electronic mail (e-mail) system by students, their parents and others and applies to any and all electronic messages composed, sent or received by anyone using the District's student e-mail system. Authorized users of e-mail are students, their parents and any other individuals or groups issued District student e-mail accounts. (See also Policy 7540.03)

I. District E-Mail

The use of e-mail as an educational and communication tool is encouraged. Users of the District e-mail services do so responsibly and comply with Florida and Federal laws, District policies and procedures, and established standards of personal and professional conduct and courtesy.

II. Acceptable Use of District E-mail Services

Use of District student e-mail system must support and be consistent with District objectives. All users must be aware of and understand the standards by which the District expects and requires users to conduct themselves. These standards are found in, among other things, the District's ~~Student~~ *Code~~s~~ of Student Conduct* (Elementary and Secondary) (Policy 5500), Policy 7540.03, and the District Network Security Standards. All users must familiarize themselves with all applicable standards. A user's failure to familiarize himself/herself with these guidelines will not constitute a viable defense or be a mitigating factor to a charge that the user has violated this policy. Student use must be strictly consistent with the District's curriculum goals and is intended for academic use only. Students shall use the system only as directed by their teacher and exclusively for class-related

work. Personal e-mail use may be permitted for other purposes only as authorized by District administration.

III. Unacceptable Use of District E-mail Services

Users may not use the District's student e-mail system to perform any action or transmit any communication that would otherwise be prohibited in any other medium of communication. This means that e-mail must follow the same rules of conduct as in face-to-face or written communications.

Unacceptable and prohibited uses include, but are not limited to:

A. Using profanity, obscenity, or other language which may be offensive to another user or any matter deemed to be obscene under the law. Obscene material is material which: 1) the average person, applying contemporary community standards, would find, taken as a whole, appeals solely to prurient interests; and 2) depicts or describes in a patently offensive way, sexual conduct as defined by State law; and 3) taken as a whole, lacks serious literary, artistic, political, or scientific value.

B. Transmitting any material that is in violation of Federal, State, and local laws, or of Board policies, standards, regulations, or guidelines. This includes, but is not limited to, unauthorized distribution of material that is obscene, pornographic, or contains statements that would tend to violate an individual's civil or constitutional rights or constitute bullying, harassment, slander, defamation, discrimination, cyberstalking, or transmission of trade secrets or copyrighted material without the consent of the owner or copyright holder. (See also Policy 7540.03)

C. "Spoofing" where spoofing is defined as the act of disguising the sender of an e-mail by replacing the name in the "from" line or header fields, sending e-mails while signed on as a different user, or otherwise intentionally misleading the recipient as to the identity of the actual sender.

D. Sending anonymous e-mail.

E. Engaging in any activity designed to view the e-mails of other individuals without authority or permission.

F. Using the District's global distribution lists is prohibited.

G. Initiating or forwarding "chain-letters" or petitions.

H. "Spamming," or the sending of unwanted, unsolicited and/or unnecessary messages to large numbers of people, usually with the purpose of advertising a product, event, service, or lobbying for a specific political position or promoting an individual's opinion. In many cases, the sender is unknown to

the recipients. The District has the right to block and/or remove any e-mail that it determines is spam.

I. Violating the Student Code of Conduct.

IV. Consequences of Inappropriate Use of District E-mail Services

The student e-mail system is the property of the District. The District may monitor the e-mail system for unacceptable use according to Federal, State, and local laws and District procedures, policies and rules. Any user who violates this policy is subject to revocation of e-mail privileges and/or appropriate disciplinary action, up to and including suspension and/or expulsion.

A. Principals, teachers and District administrators are authorized to determine whether a user is in compliance with this rule and is using the District's e-mail system in an appropriate and acceptable manner. This includes monitoring any user's e-mail for the purpose of determining compliance.

B. Students and parents must register and complete the Student E-Mail Parental Consent Form before they will be authorized to use the District e-mail system.

C. Users will be given an e-mail account and password and must sign in to use the e-mail system. Users will be held responsible for all activity associated with their account and must not share their password with anyone, with the exception that students may share their password with their parents or teacher, if necessary. Users will have the ability to change their password and must do so if the confidentiality of their password has been compromised.

D. Students will not be given access to the e-mail system without written approval from their parents/guardians. Parents/Guardians must be aware that although the District will use blocking and filtering technology and will monitor e-mail use as carefully as possible, inappropriate material may still be transmitted by their child. Parents are wholly responsible for the e-mail transmissions of their child while using the District e-mail system.

E. Students must not send any restricted or personal information, especially names, addresses and phone numbers, or communicate with non-school site personnel without the knowledge and supervision of their teacher. Students who receive unsolicited e-mails from strangers or threatening or otherwise inappropriate e-mail from anyone shall report the incident to their teacher or school administrator immediately and must not reply.

F. Users must not reply to or forward advertising e-mail, or "spam" and must delete it without opening.

G. Users are prohibited from sharing any list of the e-mail addresses of persons in their class with anyone not enrolled in the class.

H. Teachers must use due diligence and stop and/or report students they see or hear are using the e-mail system in an inappropriate manner. In particular, inappropriate uses including, but not limited to, sending obscenity, pornography, copyrighted material, test answers or the sending or forwarding of threats or bullying through the e-mail system are strictly prohibited and will result in disciplinary action.

I. Users of the student e-mail system shall not expect that e-mail generated or received via the District's e-mail system will remain private. Users must be aware that:

1. Sensitive and confidential data, including data considered exempt from public disclosure, may be viewed by persons other than the intended recipient. Information that is exempt or confidential under State and Federal law may need to be encrypted, blocked out, or not transmitted by e-mail. E-mail is legally discoverable and may be used in court proceedings.

2. Users are notified that there is no individual right to privacy in the use of the District's e-mail system. Administration has an absolute right to monitor use of the e-mail system at its discretion. Users are warned that although e-mail often has the feel of a private conversation, it is in fact, not private. (See the District's Board policy concerning privacy.)

J. The District also has the right to:

1. review e-mails stored in the District email system~~network~~ for the purpose of maintaining adequate and necessary ~~file server~~ storage space, ~~and~~to determine whether there is an imminent safety threat or the District's interests have been compromised, and to ensure appropriate use and compliance with Policies 7540.01, *Technology Privacy*, and 7540.03, *Student Responsible Use of Technology, Social Media, and District Network Security Systems & Internet Safety*,

2. modify or delete e-mails or attachments that may contain computer viruses or any other computer code that could damage or destroy any portion of the network, and~~.~~

~~2.~~3. block e-mails that violate this policy.

Effective 07.01.2011

Legal References:
F.S. 119.011~~,~~

F.S. 257.05
F.S. 668.60 et seq.
F.S. 668.701 et seq.
F.S. 748.048
F.S. Ch. 847, et. seq.
F.S. 1006.07

Adoption Date: 05.11.2011