< Prev Next >

To Regulation

Search District Policies

District Policies TOC

District Policy

2361- TELECOMMUNICATIONS/TECHNOLOGY (M)

Section: Program
Date Created: March, 2016
Date Edited: March, 2016

M

The Board shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, statewide, national and global communications opportunities for staff and students. Educational technology shall be infused into the district curriculum to maximize student achievement of the Core Curriculum Content Standards.

Educational technology shall be infused into the district curriculum to maximize student achievement of the Core Curriculum Content Standards. Beginning in the 2014/2015 school year, the district shall incorporate instruction on the responsible use of social media into the technology education curriculum for students in grades 4 through 8 as part of the implementation of the core curriculum standards.

It is the policy of the district to establish safe and effective methods for student and staff users of the district's technological resources and to:

A. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

B. Prevent unauthorized access and other unlawful online activity;

C. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

D. Comply with the Children's Internet Protection Act (CIPA).

Definitions

For the purposes of this policy, the following definitions shall apply:

1. Computer Network/Computers consist of any school managed or owned computer equipment or systems, including, but not limited to, networks, hard drives, servers, peripherals, printers, networking systems, devices, modems, all electronic documents, video, voice and data networks, routers, storage devices, and classrooms equipped with such. Computer Network/Computers shall also include electronic

communications which shall be defined as and include the use of information systems in the communicating, posting, or obtaining of information or materials by way of electronic mail, bulletin boards, Internet, or other such electronic tools.

2. User is any individual, with or without authorization, who utilizes the district's computing system from any location.

Compliance With CIPA

Filters Blocking Access to Inappropriate Material

A. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

B. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the school district online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

1. Unauthorized access, including so-called "hacking," and other unlawful activities; and

2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

C. cation, Supervision and Monitoring

It shall be the responsibility of all members of the school district staff to educate, supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the chief school administrator or his or her designee.

The Chief School Administrator or his or her designee shall ensure that students and staff who use the school internet facilities receive appropriate training including the following:

1. The district established standards for the acceptable use of the internet;

2. Internet safety rules;

3. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;

4. Cyberbullying (Board Policy 5512 Harassment, Intimidation and Bullying) awareness and response.

Student use of the Internet shall be supervised by qualified staff.

Standards for the Promotion of Online Safety for Students

While the Internet offers a variety of opportunities to enhance students' educational experiences, there are certain risks associated with the Internet created by other users. Students are required to adhere to the following guidelines regarding safety. Any individual who fails to adhere to these guidelines will have his/her network privileges revoked.

1. Users are prohibited from disclosing personal information such as addresses, phone numbers, pictures, or the name and location of the school without the permission of a teacher and a parent.

2. Users are obligated to disclose to a teacher or parent any information or electronic messages which make them uncomfortable.

3. Users shall never meet in person with someone they have met online without first receiving permission from a parent. The Board does not condone such meetings and strongly suggests that they do not occur.

4 Users shall report any security problems, such as a gap in system or network security, to a teacher or system administrator.

5. Users shall set a password for their account to protect it from unauthorized use. The password should be difficult to guess and should be changed on a regular basis to assure the continued security of the account. Users should never divulge their passwords and will be held accountable for the consequences of intentionally or negligently disseminating this information.

Acceptable Use Of The Internet

The Board recognizes that telecommunications and other new technologies will shift the manner in which information is accessed, communicated, and transferred. These new technologies will alter the nature of teaching and learning. Access to telecommunications will allow students and employees to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The Board supports access by students and employees to these information sources and

the potential they have to enhance students' educational experiences, but it reserves the right to limit use of these new technologies during school hours and on school premises to legitimate educational purposes. At all other times, the Board demands that users utilize the computer network in a responsible manner and in accordance with this policy.

The Board also recognizes that telecommunications will allow students access to information sources that have not been pre-screened by educators using Board approved standards. While the Board will make its best efforts to monitor use of school computer networks/computers, the Board cannot monitor users at all times and cannot guarantee that users will not access inappropriate materials, especially when access is from a site off campus. The Board therefore adopts the following standards of conduct for the use of computer network/computers, including electronic mail communications, to which all users are expected to adhere, and declares unethical, unacceptable and illegal behavior in violation of these standards, and said behavior will serve as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer network/computers for educational purposes only, and, for employees, for purposes related to job performance. The Board retains the right to restrict or to terminate access to the computer network/computers at any time, for any reason. The Board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and to ensure its proper use.

Standards for Use of Computer Networks

It is understood that computer networked services are provided exclusively for educational purposes. Educational purposes are those that are related to or necessary to prepare for or to complete lessons or classroom assignments, and, for employees, those purposes related to job performance. Users will adhere to the standard of conduct required in the classroom and will follow the regulations posted in the computer lab. Users are prohibited from engaging in the following conduct and shall be subject to discipline and/or legal action for such conduct:

1. Using the computer network/computers for illegal activities or in support of illegal activities. Illegal activities are defined as activities which violate federal, state, and local laws or regulations.

2. Using the computer network/computers in a way that violates existing district policy.

3. Using the computer network/computers for obscene purposes or to obtain or transmit obscene materials. Obscene materials are those that appeal to the prurient interest, depict sexual conduct in a patently offensive way, and lack serious literary, artistic, or scientific value.

4. Using the computer network/computers to send or display lewd, indecent, or vulgar speech or materials.

5. Using the computer network/computers to send or display harassing, demeaning, or offensive speech or materials.

6. Using the computer network/computers to engage in activities that could materially or substantially interfere with the operation of the school, the school's educational mission, or other students' rights.

7. Using the computer network/computers to violate copyrights, trademarks, an individual's right of publicity, any form of intellectual property, license agreements, or other contracts.

8. Displaying any personally identifiable information about students including name, address, photographs, social security number, or other personal characteristics that would make the student easily identifiable without obtaining prior parental consent. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

9. Using the computer networks/computers in a manner that:

   a. Intentionally disrupts network traffic or crashes the network;

   b. Degrades or disrupts equipment or system performance. Examples of conduct that degrade or disrupt equipment or system performance include, but are not limited to, the following activities: utilizing shared computing resources for excessive game playing or other trivial applications; sending unnecessary or excessive mail or messages; printing of excessive copies of documents, files, images or data; deliberately running grossly inefficient programs when more efficient choices are available; creating, sending, or forwarding electronic chain letters;

   c. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;

   d. Steals data or other intellectual property;

   e. Gains or seeks unauthorized access to files of others or vandalizes the data of another user;

   f. Forges electronic mail messages or uses an account owned by others; and/or creates an account under false/identity theft.

   g. Invades the privacy of others. Users will not use the network to obtain private information about others, post private information about another person, or re-post a

message that was sent to them privately without permission of the person who sent the message;

h. Posts anonymous messages;

i. Possesses any data which is in violation of this policy; and/or

j. Engages in other activities that do not advance the educational purposes for which the computer network/computers are provided.

k. Uses outside software without the prior approval of the school's technology coordinator or system administrator.

Off school premises, users may utilize the computer network for legitimate, non-education related reasons. However, users are expected to adhere to this policy in all other regards, and specifically, shall adhere to the user guidelines set forth above.

Users will be personally charged for any unauthorized costs incurred in their use of the computer network/computers and held responsible for any damages caused by their intentional misuse of the computer network/computer equipment.

Users are required to report any evidence of a violation of these rules to school authorities and employees are expected to ensure to the best of their abilities that students use the computer network/computers in accordance with this policy.

The district will fully cooperate with any local, state or federal agency in any investigation concerning or relating to misuse of the district's computer network/computers.

Aside from this policy, use of the computer network/computers by students and employees will be governed by the district's existing policies and, for employees, the existing Collective Bargaining Agreement specifically as it relates to professional conduct.

Any violation of district policy and rules may result in a loss of district-provided access to the Internet. Violations may result in additional disciplinary action, including suspension and expulsion. When applicable, law enforcement agencies will be contacted regarding potential illegal activities. Specifically, individuals violating this policy shall be subject to appropriate discipline which could include, but which is not limited to:

a. Use of network only under direct supervision;

b. Suspension of network privileges;

c. Revocation of network privileges;

d. Suspension of computer privileges;

e. Revocation of computer privileges;

f. For students, suspension or expulsion from school;

g. For employees, letters of reprimand, increment withholding, loss of employment; and/or

h. Legal action and prosecution by the authorities.

Privacy

Individuals should have no expectation of privacy with respect to their files on Board provided computer network/computers. All data stored or transmitted or accessed by users, including E-mail, can and will be monitored by the Board.

Due Process

In the event there is an allegation that a student has violated the Acceptable Use Policy, that student will be provided with a written notice of the alleged violation and an opportunity to present an explanation before a district administrator. A hearing will be provided when required by district policy or the applicable statutes and regulations governing discipline of students.

Employee violations of the Acceptable Use Policy will be handled in accordance with district policy and the current Collective Bargaining Agreement.

Intellectual Property and Plagiarism

Because certain works found on the Internet are protected by copyright, trademark, and other forms of intellectual property, employees will either request permission from the owner of the intellectual property rights prior to using any materials obtained on the Internet, or the employee will consult with the administration to determine whether the materials may be used without receiving permission based on certain exceptions to intellectual property rights as set forth in the relevant laws. Teachers will instruct students to adhere to the same guidelines.

Users will be held personally liable for any of their own actions that violate another party's intellectual property rights. District practices on plagiarism will govern the use of materials accessed through the Internet. Teachers will instruct students as to the definition of plagiarism and the proper method to cite to materials.

Responsibility for Damage Suffered

The Demarest Public School District makes no warranties of any kind, expressed or implied, for the Internet access it provides. The district will not be responsible for any damage users suffer including, but not limited to, loss of data or interruption of service. The district will also not be responsible for the accuracy or quality of the information obtained through or stored on the system. The Board will not be responsible for financial obligations arising from the unauthorized use of the system.

District Web Site

The Chief School Administrator shall publish and disseminate guidelines on acceptable material for district web sites. The Chief School Administrator shall also ensure that district and school web sites do not disclose personally identifiable information about students without prior written consent from parents/guardians. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers, and locations and times of class trips.

Parental Notification and Responsibility

The chief school administrator shall ensure that parents/guardians are notified about the district network and the rules governing its use. No student will be permitted to use the district's telecommunications system unless and until the student and his/her parents (if the student is less than 18 years old) sign the district's Consent and Release Form which acknowledges that:

A. The student and his/her parent, if applicable, have read and understand this policy and the accompanying regulation;

B. The student will be held accountable for all of his/her network and Internet activities;

C. The student is expected to comply with the district's policy and regulation and all federal, state and local laws governing Internet use; and

D. The student and his/her parent shall indemnify and hold harmless the Demarest Board of Education, its members, agents, servants and employees from any and all liability relating to the student's use of the district's telecommunications system or the Internet.

Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Consent Requirement

No student shall be allowed to use the district-provided computer network unless they have filed an executed consent form with the principal. Guests to the school must also sign a consent form. Consent forms are available from the main office. Anyone using the system without first executing a consent form will be deemed to have consented to the principles embodied in this policy.

Policy Development

The district Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

Implementation

The Chief School Administrator shall prepare regulations to implement this policy.

Bring Your Own Device Statement

If a student elects not to receive a school-issued computer, he/she may provide their own device that meets minimum specifications that are to be set and revised by administration every two years. The minimum specifications for devices are listed below:

Platform/OS	MacBook Pro (Early 2011 model) OR MacBook Air (Mid 2012 model) with OS X v10.9 Mavericks
Display	13-inch MacBook Pro OR 11-inch MacBook Air
Local Storage	128 GB
Memory	8 GB
Audio/Video/ Peripherals/ Wireless	3.5mm stereo headphone mini input, internal microphone, USB, Thunderbolt, Wi-Fi, Bluetooth, and Face Time HD camera must be in normal working condition
Battery Health	Cycle Count less than 1000 and Normal Condition
Protective Case	Hard shell protective cover and/or case
Accessories	Stereo headphones are to be provided by the student to promote good hygiene

Each student and parent must complete required training prior to bringing their equipment to class. In addition, students must comply with the policy for personal electronic devices, which are as follows:

1. The student is responsible for keeping his/her device in their possession and properly securing it at all times. District personnel are not responsible for the security or condition of student's personal devices.

2. The student is responsible for the proper care of school-issued laptops. This includes proper care, safety, and functionality.

3. The district reserves the right to confiscate and/or inspect personal technology devices if there is reason to believe that it was used to violate our policies, administrative procedures, school rules, or for general misconduct.

4. Violations may result in the loss of privilege to use personal technology in school, and/or disciplinary and legal action, as appropriate.

5. The student must comply with the teachers' request to refrain from using a device or to power down (turn off) the device. The student should only use personal technology devices with

consent and under the direct supervision of a district faculty member.

6. The student may not use any devices to record, transmit, or post photos or videos of any person without their knowledge and consent. Images, video and audio files recorded at school may not be transmitted or posted at any time without the expressed permission of a district faculty member.

7. All users are required to utilize The District's secured wireless network to access the Internet while on school grounds. The use of private wireless Internet connections is not allowed during school hours. Students are allowed to set up wireless networks on school-issued electronic devices at home only. Parents/guardians are responsible for monitoring Internet use at home.

8. The student must allow for District installation of software and user profiles that may be required to access the computer network, to install software, to filter content, and/or for test administration.

9. The District shall not be responsible for damages to devices brought from home. Parents/guardians may refer to homeowner's insurance coverage for damages and theft coverage. Accidents, vandalism, or theft must be reported to the appropriate technician or administrator within one school day following the incident.

Anti-Big Brother Statement

The Statute (NJ Legislature) states the following:

CHAPTER 44: AN ACT concerning notification to certain persons using certain electronic devices and supplementing Title 18A of the New Jersey Statutes.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey: C.18A:36-39 Notification by school to certain persons using certain electronic devices; fine. 1.A school district or charter school that furnishes a student with a laptop computer, cellular telephone, or other electronic device shall provide the student with written or electronic notification that the electronic device may record or collect information on the student's activity or the student's use of the device if the electronic device is equipped with a camera, global positioning system, or other feature capable of recording or collecting information on the student's activity or use of the device. The notification shall also include a statement that the school district or charter school shall not use any of the capabilities in a manner that would violate the privacy rights of the student or any individual residing with the student. The parent or guardian of the student shall acknowledge receipt of the notification. The school district or charter school shall retain the acknowledgement as long as the student retains the use of the electronic device.

Demarest Public Schools will furnish each student with an Apple laptop. We understand that the iMac is an Internet connected device that is equipped with a camera, Global Positioning System, and/or other feature capable of recording or collecting information on the student's activity or use of the device. Demarest Public Schools "shall not use any of the capabilities of the laptop in a manner that would violate the privacy rights of the student or any individual residing with student."

Receiving and Registering Your Computer

All school-issued computers will display a serial number, which will be registered to a specific student. All students are responsible for the computer registered to them. Students who choose to use their own device must provide a letter of intention to use their own technology to the building administration. Letters of intention should be given to the school principal. All students must use The District filtered wireless network while on school grounds. By authenticating and logging into The District network, the student is agreeing to comply with the terms of The District Acceptable Use Policy (AUP). Once on The District network, all users will have filtered Internet access on their personal equipment in compliance with the Children's Internet Protection Act (CIPA), just as they would on District devices.

School-Issued Technology Insurance

Our vision is to equip each student with a laptop to be used for enhancing the learning experience and enriching curricular content. All middle school students will have access to a laptop for the school year. However, in order for students to take their laptop home and make it a truly personal device, which is the intended function of the Apple hardware, insurance must be purchased.

The laptop insurance will cost approximately $85.00 for each unit. The protection plan will cover theft, accidental damage, drops, liquid spills and submersion, cracked screens, mechanical breakdowns, and manufacturer defects. It also allows transfer of coverage to a new device should the laptop need replacement. Insurance will not cover deliberate misuse or neglect of any school-issued laptop.

The laptops are the property of The Demarest Board of Education. Any student that does not purchase insurance will not be allowed to take a laptop outside of the school building. The student will be responsible to pay for any and all damages that occur during school use. In the event that a student does not purchase insurance, the student's family will be responsible to pay for any and all damages that occur to the laptop during school use. The Demarest Board of Education highly recommends purchasing insurance to protect student-issued laptops. If a family is unable to pay for insurance please contact the school principal.

Technology and Computer Use At School and Home

The District will allow students to bring their own authorized technology devices (currently includes laptops, netbooks, eReaders, iPads, and android tablets) for personal use at the following specified times during the school day:

1. Before/after school; and

2. In the classroom, when specifically permitted by the classroom teacher.

Students and staff are required to access The District's wireless network when using the approved devices during the school day under the supervision of the classroom teacher or when authorized to use approved devices for personal use as approved by the school principal. While users may operate their own devices to access the Internet, they must do so by way of the district's filtered wireless connections. The use of private Internet access on school grounds is prohibited. Users may not disable, override or circumvent district technology filters, profiles nor other provisioning/protection measures.

The student-issued laptop shall remain property of The Demarest Board of Education. Students are responsible for adhering to the guidelines and rules set forth by Demarest Middle School. Students are responsible for the general care of the laptop, case and charger.

1. Do not place any stickers on the laptop, case, or cover. Do not write or draw on the laptop, case, or cover. The case must remain on school-issued laptops at all times.

2. Carefully insert and remove cords and cables from the laptop to prevent damage and/or loss of data.

3. Do not leave your laptop in an unsupervised area, hot or frigid car or by fluids. When not using your laptop it should be safely locked in your locker.

4. Laptops are not allowed in the cafeteria during lunchtime, unless the school principal grants special permission. Please keep laptops away from food and drinks both in and out of school.

5. The profile settings in place are to remain the same. Any alterations in these settings could result in loss of laptop privileges.

6. Students will be given a default password and will then create a new one upon being issued the device. This password is NEVER to be changed. Students should NEVER share their password with a peer.

7. The act of "jail breaking" a piece of hardware or software involves hacking the device and bypassing restrictions set fort by the manufacturer/creator in order to run "unauthorized" software and/or make changes to the operating system. This practice is not allowed. All laptops, the pre-installed operating system, and software must remain in original condition.

The Demarest Middle School can restrict or disable any functions, hardware components, software, or apps which do not support classroom instruction, curricular content or positive interaction among peers.

The District Acceptable Use Policy governs laptop use. Any infraction of this policy can lead to a suspension of technology rights and/or appropriate discipline as directed by the school principal. Laptops can be collected at any time for software updates or general inspection.

Taking Care of Your Electronic Equipment

Students who are provided with a school-issued laptop must comply with the following regulations provided below. All devices are school property and all users of these devices must adhere to the safety and care instructions implemented through the Acceptable Use Policy for Technology.

A. Clean the screen with a soft, dry cloth or anti-static cloth. Use of harsh chemicals will damage the screen.

B. Cords and cables must be inserted carefully into the computer device to prevent damage.

C. The school-furnished electronic device and case must remain free of any writing, drawing, stickers, or labels that are not the property of Demarest Board of Education.

D. School-furnished electronic device must never be left in an unlocked locker, unlocked car, or any unsupervised area.

E. Students are responsible for keeping the battery charged and computer ready for school each day. Teachers are permitted to deny technology use if the computer is not charged.

F. The protective cases with sufficient padding shall be provided to protect the device from normal treatment and provide a suitable means for carrying the device within the school. Students must keep their school-furnished electronic device in the protective case, provided by the school, at all times.

All school-issued computers must be handled carefully and properly to prevent damages.

1. Do not lean on the top of the electronic device when it is closed.

2. Do not place anything near the electronic device that could put pressure on the screen.

3. Do not place anything in the carrying case that will press against the cover.

4. Do not “bump” the electronic devices against lockers, walls, car doors, floors, etc. as it will eventually break the screen.

Damages, Repairs, and Maintenance

All damages to school-issued devices must be reported to the main office immediately. In cases of theft, loss or vandalism, students or parents must file

a police report and bring a copy of the report to the Principal's office before a new device can be issued.

Students will be responsible for damages to their school-issued electronic devices including, but not limited to, broken screens, cracked plastic pieces, inoperability, etc. In the case of intentional damage and/or neglect, should the cost to repair exceed the cost of purchasing a new device, the student will pay for full replacement value. If the repair cost does not exceed the cost of replacement, the student will be responsible to pay for the damages in full. Lost items, such as sleeves and cables, and any additional accessory items, will be charged the actual replacement cost.

Damages, Repairs, and Maintenance

All damages to school-issued devices must be reported to the main office immediately. In cases of theft, loss or vandalism, students or parents must file a police report and bring a copy of the report to the Principal's office before a new device can be issued.

Students will be responsible for damages to their school-issued electronic devices including, but not limited to, broken screens, cracked plastic pieces, inoperability, etc. In the case of intentional damage and/or neglect, should the cost to repair exceed the cost of purchasing a new device, the student will pay for full replacement value. If the repair cost does not exceed the cost of replacement, the student will be responsible to pay for the damages in full. Lost items, such as sleeves and cables, and any additional accessory items, will be charged the actual replacement cost.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act
Federal Communications Commission: Neighborhood Children's Internet Protection Act

Adopted: 22 March 2016

< Prev Next >

To Policy

Search District Regulations
District Regulations TOC

District Regulation

2361 - ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

Section: Program
Date Created: March, 2016
Date Edited: March, 2016

The school district provides computer equipment, computer services, and Internet access to its students and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources.

For the purpose of this Policy and Regulation, "computer networks/computers" includes, but is not limited to, the school district's computer networks, computer servers, computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment.

For the purpose of this Policy and Regulation, "school district personnel" shall be the person(s) designated by the Superintendent of Schools to oversee and coordinate the school district's computer networks/computer systems. School district personnel will monitor networks and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate Internet safety.

Due to the complex association between government agencies and computer networks/computers and the requirements of Federal and State laws, the end user of the school district's computer networks/computers must adhere to strict regulations. Regulations are provided to assure staff, community, students, and parent(s) or legal guardian(s) of students are aware of their responsibilities. The school district may modify these regulations at any time. The signatures of the student and his/her parent(s) or legal guardian(s) on a district-approved Consent and Waiver Agreement are legally binding and indicate the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules and regulations established under Policy and Regulation **2361**.

Students are responsible for acceptable and appropriate behavior and conduct on school district computer networks/computers. Communications on the computer networks/computers are often public in nature and policies and regulations governing appropriate behavior and communications apply. The school district's networks, Internet access, and computers are provided for students to conduct research, complete school assignments, and communicate with others. Access to computer networks/computers is given to students who agree to act in a considerate, appropriate, and responsible manner. Parent(s) or legal guardian(s) permission is required for a student to access the school district's computer networks/computers. Access entails responsibility and

individual users of the district computer networks/computers are responsible for their behavior and communications over the computer networks/computers. It is presumed users will comply with district standards and will honor the agreements they have signed and the permission they have been granted. Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer networks/computers who violate the policies and regulations of the Board.

Computer networks/computer storage areas shall be treated in the same manner as other school storage facilities. School district personnel may review files and communications to maintain system integrity, confirm users are using the system responsibly, and ensure compliance with Federal and State laws that regulate Internet safety. Therefore, no person should expect files stored on district servers will be private or confidential.

The following prohibited behavior and/or conduct using the school district's networks/computers, includes but is not limited to, the following:

1. Sending or displaying offensive messages or pictures;

2. Using obscene language and/or accessing material or visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;

3. Using or accessing material or visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;

4. Using or accessing material or visual depictions that are harmful to minors including any pictures, images, graphic image files or other material or visual depictions that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

5. Depicting, describing, or representing in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors;

6. Cyberbullying;

7. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;

8. Harassing, insulting, or attacking others;

9. Damaging computers, computer systems, or computer networks/computers;

10. Violating copyright laws;

11. Using another's password;

12. Trespassing in another's folders, work or files;

13. Intentionally wasting limited resources;

14. Employing the computer networks/computers for commercial purposes; and/or

15. Engaging in other activities that do not advance the educational purposes for which computer networks/computers are provided.

INTERNET SAFETY

Compliance with Children's Internet Protection Act

As a condition for receipt of certain Federal funding, the school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter material or visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, 4, 5, 6, and 7 above and in the Children's Internet Protection Act. The school district will certify the schools in the district, including media centers/libraries are in compliance with the Children's Internet Protection Act and the district complies with and enforces Policy and Regulation **2361**.

Compliance with Neighborhood Children's Internet Protection Act

Policy **2361** and this Regulation establish an Internet safety protection policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web;

2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

3. Unauthorized access, including "hacking" and other unlawful activities by minors online;

4. Cyberbullying;

5. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;

6. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and

7. Measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding the material or visual depictions defined in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine Internet material that is inappropriate for minors.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety protection policy - Policy and Regulation **2361**. Any changes in Policy and Regulation **2361** since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

Information Content and Uses of the System

Students may not publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane, or sexually offensive to a reasonable person, or which, without the approval of the Superintendent of Schools or designated school district personnel, contains any advertising or any solicitation to use goods or services. A student cannot use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity which is prohibited by law.

Because the school district provides, through connection to the Internet, access to other computer systems around the world, students and their parent(s) or legal guardian(s) should be advised the Board and school district personnel have no control over content. While most of the content available on the Internet is not offensive and much of it is a valuable educational resource, some objectionable material exists. Even though the Board provides students access to Internet resources through the district's computer networks/computers with installed appropriate technology protection measures, parents and students must be advised potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school district.

Students and their parent(s) or legal guardian(s) are advised some systems and Internet sites may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material. The Board and school district personnel do not condone the use of such materials and do not permit usage of such materials in the school environment. Parent(s) or legal guardian(s) having Internet access available to their children at home should be aware of the existence of such materials and monitor their child's access to the school district system at home. Students knowingly bringing materials prohibited by Policy and Regulation **2361** into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such students' accounts or access on the school district's computer networks and their independent use of computers.

On-line Conduct

Any action by a student or other user of the school district's computer networks/computers that is determined by school district personnel to constitute an inappropriate use of the district's computer networks/computers or to improperly restrict or inhibit other persons from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending person's access and other consequences in compliance with Board policy and regulation. The user specifically agrees not to submit, publish, or

display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, State or Federal law is also prohibited and is a breach of the Consent and Waiver Agreement.

Students and their parent(s) or legal guardian(s) specifically agree to indemnify the school district and school district personnel for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the student.

Computer networks/computer resources are to be used by the student for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network

Software libraries on or through the school district's networks are provided to students as an educational resource. No student may install, upload, or download software without the expressed consent of appropriate school district personnel. Any software having the purpose of damaging another person's accounts or information on the school district computer networks/computers (e.g., computer viruses) is specifically prohibited. School district personnel reserve the right to refuse posting of files and to remove files. School district personnel further reserve the right to immediately limit usage or terminate the student's access or take other action consistent with the Board's policies and regulations of a student who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without authorization. Students may download copyrighted material for their own use in accordance with Policy and Regulation 2531 - Use of Copyrighted Materials. A student may only redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author or authorized source.

Public Posting Areas (Message Boards, Blogs, Etc.)

Messages are posted from systems connected to the Internet around the world and school district personnel have no control of the content of messages posted from these other systems. To best utilize system resources, school district personnel will determine message boards, blogs, etc. that are most applicable to the educational needs of the school district and will permit access to these sites through the school district computer networks. School district personnel may remove messages that are deemed to be unacceptable or in violation of Board policies and regulations. School district personnel further reserve the right to immediately terminate the access of a student who misuses these public posting areas.

Real-time, Interactive, Communication Areas

School district personnel reserve the right to monitor and immediately limit the use of the computer networks/computers or terminate the access of a student who misuses real-time conference features (talk/chat/Internet relay chat).

Electronic Mail

Electronic mail ("email") is an electronic message sent by or to a person in correspondence with another person having Internet mail access. The school district may or may not establish student email accounts. In the event the district provides email accounts, all messages sent and received on the school district computer networks/computers must have an educational purpose and are subject to review. Messages received by a district-provided email account are retained on the system until deleted by the student or for a period of time determined by the district. A canceled account will not retain its emails. Students are expected to remove old messages within fifteen days or school district personnel may remove such messages. School district personnel may inspect the contents of emails sent by a student to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, State, or Federal officials in any investigation concerning or relating to any email transmitted or any other information on the school district computer networks/computers.

Disk Usage

The district reserves the right to establish maximum storage space a student receives on the school district's system. A student who exceeds his/her quota of storage space will be advised to delete files to return to compliance with the predetermined amount of storage space. A student who remains in noncompliance of the storage space allotment after seven school days of notification may have their files removed from the school district's system.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a student identifies a security problem on the computer networks/computers, the student must notify the appropriate school district staff member. The student should not inform other individuals of a security problem. Passwords provided to students by the district for access to the district's computer networks/computers or developed by the student for access to an Internet site should not be easily guessable by others or shared with other students. Attempts to log in to the system using either another student's or person's account may result in termination of the account or access. A student should immediately notify the Principal or designee if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any student identified as a security risk will have limitations placed on usage of the computer networks/computers or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism to any school district owned computer networks/computers may result in cancellation of system privileges and other disciplinary measures in

compliance with the district's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer networks/computers that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer networks/computers should be used judiciously. Unauthorized printing for other than educational purposes is prohibited.

Internet Sites and the World Wide Web

Designated school district personnel may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by designated school district personnel who shall ensure the content of the site complies with Federal, State, and local laws and regulations as well as Board policies and regulations.

Violations

Violations of the Acceptable Use of Computer Networks/Computers and Resources Policy and Regulation may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and/or Regulation, **2361** - Acceptable Use of Computer Networks/Computers and Resources, 5600 - Student Discipline/Code of Conduct, 5610 - Suspension and 5620 - Expulsion as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this Policy shall be determined by the Principal or designee. The Superintendent or designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities is the appropriate course of action.

Individuals violating this Policy shall be subject to the consequences as indicated in Board Policy and Regulation **2361** and other appropriate discipline, which includes but is not limited to:

1. Use of computer networks/computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;

7. Expulsion from school; and/or

8. Legal action and prosecution by the authorities.

Issued: 22 March 2016