2360 USE OF TECHNOLOGY

The Board of Education recognizes the use of technology in the educational process is an essential part of the schooling experience. Technology is to be viewed as a resource to enhance the learning process among other resources available to teachers and pupils. In addition, technology can be used to enhance the administration of the school. In order to provide direction and meaning to the use of technology as an instructional resource, the Board encourages and supports staff use of technology as a component of the learning process.

For purposes of this policy "technology" includes, but is not limited to, the use of computers and computer peripherals, communications networks, access to databases and libraries of information and the integration of audio, video, multimedia devices and media for purposes of teaching and learning.

The Superintendent, in consultation with teaching and support staff, shall recommend to the Board the acquisition of appropriate technology to best implement the curricular, instructional, and administrative program of the school district. The Superintendent shall prepare a technology plan for the school district to encompass the following:

Curricular, Instructional and Administrative Need

The technology plan shall define the curricular, instructional and administrative need for technological equipment and media for the district.

In-service Education

The Board shall provide opportunities for school staff to participate in in-service programs on hardware or software programs to be used in the execution of educational and administrative tasks. In-service programs may be provided in or out of the district.

Standards, Codes and References

All technology installations shall conform to the industry standards and applicable federal, State and local statutes and codes.

Facilities Planning

In all facilities projects involving new constructions, additions, and renovations the Superintendent or designee shall ensure the plans include provisions for current and future technology needs in terms of the structural, electric/electronic, mechanical, acoustical and visual systems of the building(s). All educational specifications shall include features required for the use of instructional technology.

Computers

The school district will provide support or maintenance agreements for specified brands of computers. All other computers purchased or donated will be subject to repair only when non-allocated funding is available and therefore may remain unrepaired until funding is available.

Computer Software Acquisition and Upgrading

The school district will only support the specified upgrades and training. Staff members shall not purchase software that has not been included on a list of specified software or has been approved by the Superintendent and Technology Director.

The Superintendent will recommend the purchase of upgrades to software as needed. An evaluation of upgrades shall be made by appropriate personnel and no upgrade shall be purchased without the express approval of the Superintendent and Technology Director.

Site Licenses

In the case where more than one copy of a software program is required, the Technology Director shall attempt to acquire or negotiate a site license with the software developers. In the event a site license is not possible, vendors shall be sought who will provide multiple copies at a discounted cost.

Software Copyright

All employees shall strictly adhere to the copyright laws of the United States. No software shall be copied and/or distributed except in accordance with these laws. All software placed on media workstations or any network with public access shall be copy protected by the Technology Director, who shall assure that individuals who have access to such programs shall not copy them without authorization.

Internal Communication (District)

The school district shall provide communication by a variety of means.

External Communications

The Board encourages the use of external communications so the school may utilize the vast resources of external databases and communicate with other schools, external agencies, and businesses throughout the world. Gateways to such communications will be supported by the school district. The use of particular gateways shall be approved by the Technology Director. The Technology Director shall be responsible for the installation of software in district owned computers and/or computer systems that prevents access to gateways and Internet sites that have material considered by the Technology Director to be inappropriate for use by pupils.

Computer Laboratories and Distributed Computing

In order to provide teacher, staff, and pupil access to computers, the Board directs that provisions be made to provide computer access in computer laboratories, classrooms, and school libraries/media centers.

Audio/Video

All audio and/or video materials shall be used in accordance with the copyright laws of the United States. Teachers, pupils, or staff who create audio or video materials containing the voices or images of the individuals involved shall obtain proper releases from those individuals, their parent(s) or legal guardian(s) for instructional use within the school.

Informing Parents, Legal Guardians and Interested Parties

Upon request, the Building Principal shall make available to parent/legal guardians the computer hardware and software used in the district in order that a computer purchased privately for home use may be compatible with the computer and software the pupil uses in the school setting.

Technology Coordination

The Board shall appoint a Technology Director to assure the technology needs of the district are met in the most efficient manner possible at the lowest costs available to meet specified needs.

Broadcast Rights and Copyrights

The Board specifically retains the Broadcast rights and copyrights to all materials created by employees of the Board as part of their responsibilities to the Board. Any financial remuneration for the use of such materials shall be retained by the Board.

Computer Security

The Technology Director shall develop security procedures to include, but not be limited to, the following areas:

1. Physical Security of Equipment

   All computer equipment shall be maintained in a secure manner appropriate to its location.

2. Data Security

   a. Back-up procedures for system files, libraries, and data shall be practiced in a timely fashion.

   b. Disaster recovery plans shall be kept up-to-date at all times.

   c. Password protection shall be in place and updated periodically.

   d. Resource security shall be in place to prevent unauthorized access to system files, libraries, and data.

3. Employee Training

   All new employees having, as part of their job responsibilities, access to computers and information systems will be trained in the proper security procedures outlined above.

   All employees having, as part of their job responsibilities, access to computers and information systems will be kept up-to-date on current security procedures for equipment and data.

4. Transaction Audit Trail

   Appropriate procedures will be maintained in order to monitor system activity and users, as necessary.

5. Security Officer

   The Superintendent shall designate the Technology Director as the district's Computer Security Officer to monitor system security procedures.

Use of Facsimile (FAX) Machines

Fax machines provide a useful means of communicating and shall be subject to the same rules that apply to the use of telephones. All incoming faxes shall be considered confidential mail. No disclosure of the contents of any fax shall be made except to the individual for whom the fax is intended. Any individual violating this confidentiality shall be subject to discipline as provided by the policies and regulations of the Board.

N.J.A.C. 6A:26-6.1 et seq.
17 U.S.C. 101 et seq.

Adopted: 14 October 2015

2361 ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

The Board of Education recognizes as new technologies shift the manner in which information is accessed, communicated, and transferred; these changes will alter the nature of teaching and learning. Access to technology will allow pupils to explore databases, libraries, Internet sites, and bulletin boards while exchanging information with individuals throughout the world. The Board supports access by pupils to these information sources but reserves the right to limit in-school use to materials appropriate for educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes technology allows pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable, or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer networks/computers for educational purposes only. The Board retains the right to restrict or terminate pupil access to computer networks/computers at any time, for any reason. School district personnel will monitor networks and online activity to maintain the integrity of the networks, ensure their proper use, and ensure compliance with Federal and State laws that regulate Internet safety.

Standards for Use of Computer Networks

Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

A. Using the computer networks/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate Federal, State, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the networks. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.

B. Using the computer networks/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

C. Using the computer networks in a manner that:

1. Intentionally disrupts network traffic or crashes the network;
2. Degrades or disrupts equipment or system performance;
3. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;
4. Steals data or other intellectual property;
5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another person;
6. Gains or seeks unauthorized access to resources or entities;
7. Forges electronic mail messages or uses an account owned by others;
8. Invades privacy of others;
9. Posts anonymous messages;
10. Possesses any data which is a violation of this Policy; and/or
11. Engages in other activities that do not advance the educational purpose for which computer networks/computers are provided.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents 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.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

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

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure education is provided to every pupil regarding appropriate online behavior, including pupils interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

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 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.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

Consent Requirement

No pupil shall be allowed to use the school districts' computer networks/computers and the Internet unless they have filed a consent form signed by the pupil and his/her parent(s) or legal guardian(s).

Violations

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

1. Use of the network 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.

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: 14 October 2015

R 2361 ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

The school district provides computer equipment, computer services, and Internet access to its pupils 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, pupils, and parent(s) or legal guardian(s) of pupils are aware of their responsibilities. The school district may modify these regulations at any time. The signatures of the pupil 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.

Pupils 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 pupils to conduct research, complete school assignments, and communicate with others. Access to computer networks/computers is given to pupils who agree to act in a considerate, appropriate, and responsible manner. Parent(s) or legal guardian(s) permission is required for a pupil 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

Pupils 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 pupil 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, pupils 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 pupils access to Internet resources through the district's computer networks/computers with installed appropriate technology protection measures, parents and pupils must be advised potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school district.

Pupils 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. Pupils 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 pupils' accounts or access on the school district's computer networks and their independent use of computers.

On-line Conduct

Any action by a pupil 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.

Pupils 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 pupil.

Computer networks/computer resources are to be used by the pupil 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 pupils as an educational resource. No pupil 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 pupil's access or take other action consistent with the Board's policies and regulations of a pupil who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without authorization. Pupils may download copyrighted material for their own use in accordance with Policy and Regulation 2531 - Use of Copyrighted Materials. A pupil 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 pupil 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 pupil 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 pupil 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 pupil or for a period of time determined by the district. A canceled account will not retain its emails. Pupils 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 pupil 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 pupil receives on the school district's system. A pupil 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 pupil 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 pupil identifies a security problem on the computer networks/computers, the pupil must notify the appropriate school district staff member. The pupil should not inform other individuals of a security problem. Passwords provided to pupils by the district for access to the district's computer networks/computers or developed by the pupil for access to an Internet site should not be easily guessable by others or shared with other pupils. Attempts to log in to the system using either another pupil's or person's account may result in termination of the account or access. A pupil 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 pupil 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 - Pupil 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: 14 October 2015